service manual

hp StorageWorks edge switch 2/12

Product Version: FW V05.05.00-12

First Edition (November 2003)

Part Number: AA-RURDA-TE

This manual describes diagnostic, repair, and removal and replacement procedures for field replaceable units (FRUs) for the HP StorageWorks Edge Switch 2/12.

© Copyright 2003 Hewlett-Packard Development Company, L.P.

Hewlett-Packard Company makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard. The information contained in this document is subject to change without notice.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

Hewlett-Packard Company shall not be liable for technical or editorial errors or omissions contained herein. The information is provided "as is" without warranty of any kind and is subject to change without notice. The warranties for Hewlett-Packard Company products are set forth in the express limited warranty statements for such products. Nothing herein should be construed as constituting an additional warranty.

Printed in the U.S.A.

Edge Switch 2/12 Service Manual
First Edition (November 2003)
Part Number: AA-RURDA-TE

contents

About this Guide 9
Overview 10
Intended Audience 10
Related Documentation 10
Conventions 11
Document Conventions 11
Text Symbols 11
Equipment Symbols 12
Rack Stability 13
Getting Help 14
HP Technical Support 14
HP Storage Website 14
HP Authorized Reseller 14

1 General Information 15
Switch Description 15
Error-Detection, Reporting, and Serviceability Features 17
Software Diagnostic Features 18
EWS Interface 18
SNMP Trap Message Support 20
Maintenance Approach 21
Tools and Test Equipment 22
Tools Supplied with the Switch 22
Tools Supplied by Service Personnel 23
Additional Information 24

2 Diagnostics 25
Maintenance Analysis Procedures 25
Factory Defaults 25
Quick Start 26

MAP 0000: Start MAP 30
MAP 0100: Power Distribution Analysis 41
MAP 0200: POST Failure Analysis 44
MAP 0300: Loss of Web Browser PC Communication 46
MAP 0400: FRU Failure Analysis 52
MAP 0500: Port Failure and Link Incident Analysis 57
MAP 0600: Fabric, ISL, and Segmented Port Problem Determination 74

3 Repair Information 87
Procedural Notes 88
Using Log Information 89
Obtain Port Diagnostic Information 90
Port LEDs 90
EWS Interface 92
Port List Page 92
Port Stats Page 94
Port Properties Page 97
Perform Port Diagnostic Loopback Tests 98
Internal Loopback Test 99
External Loopback Test 100
Collect Maintenance Data 102
Set the Switch Online or Offline 104
Set Online State 104
Set Offline State 105
Block or Unblock a Port 106
Block a Port 106
Unblock a Port 107
Clean Fiber-Optic Components 108
Power-On Procedure 109
Power-Off Procedure 110
IML or Reset the Switch 111
Switch IML 111
Switch Reset 112
Manage Firmware Versions 113
Determine Switch Firmware Version 113
Add a Firmware Version to the Browser PC Hard Drive 114
Download a Firmware Version to the Switch 115
Reset Configuration Data 118

4 Optical Transceiver Removal and Replacement 121
Procedural Notes 121
Remove and Replace an SFP Optical Transceiver 122
Tools Required 122
Removal 122
Replacement 123

5 Illustrated Parts Breakdown 125
Front-Accessible FRUs 126
Miscellaneous Parts 127

A Event Codes 129
System Events (000 through 199) 131
Fan Module Events (300 through 399) 148
CTP Card Events (400 through 499) 151
Port Events (500 through 599) 158
Thermal Events (800 through 899) 167

Index 169

Figures

1 Edge Switch 2/12 16
2 EWS interface: View panel 18
3 Multi-mode and single-mode loopback plugs 22
4 Fiber-optic protective plug 22
5 Null modem cable 23
6 View panel (EWS interface) 31
7 View panel (Port Properties tab) 34
8 View panel (FRU Properties tab) 36
9 Monitor panel (Log page) 37
10 Connection Description dialog box 49
11 Connect To dialog box 49
12 COMn Properties dialog box 50
13 Edge-12 - HyperTerminal dialog box 51
14 Disconnect message box 51
15 Save Session message box 51
16 Monitor panel (Log page) 89
17 Monitor panel (Port List page) 93
18 Monitor panel (Port Stats page) 94

19 View panel (Port Properties page) 97
20 Operations panel (Port page with Diagnostics tab) 99
21 Operations panel (Maintenance page with Dump Retrieval tab) 102
22 Save As dialog box. 103
23 Operations panel (Switch page with Online State tab) 104
24 Configure panel (Ports page) 106
25 Clean fiber-optic components 108
26 View panel (Unit Properties page). 113
27 Operations panel (Maintenance page with Firmware Upgrade tab 115
28 Browser-specific message box. 116
29 Firmware Received message box. 116
30 Firmware Upgrade Complete message box 117
31 Operations panel (Switch page with Reset Config tab) 119
32 Browser-specific message box. 119
33 Front-accessible FRUs 126
34 Miscellaneous parts 127

Tables

1 Document Conventions 11
2 Factory-Set Defaults. 25
3 MAP Summary. 26
4 Event Codes versus Maintenance Action. 26
5 MAP 0200 Event Codes. 45
6 MAP 0200 Byte 0 FRU Codes. 45
7 MAP 400 Event Codes. 52
8 MAP 500 Event Codes. 57
9 Port Operational States and Actions 60
10 Invalid Attachment Reasons and Actions 65
11 MAP 600 Event Codes. 75
12 Port Segmentation Reasons and Actions 76
13 Byte 4 Segmentation Reasons and Actions 79
14 Bytes 8 through 11 Failure Reasons and Actions 85
15 Port Operational States. 90
16 Front-Accessible FRU Parts List 126
17 Miscellaneous Parts 127
18 Event Code 011 131
19 Event Code 021 131
20 Event Code 031 132

21 Event Code 051 132
22 Event Code 052 133
23 Event Code 061 134
24 Event Code 062 134
25 Event Code 063 135
26 Event Code 070 135
27 Event Code 071 137
28 Event Code 072 138
29 Event Code 073 138
30 Event Code 074 139
31 Event Code 080 139
32 Event Code 081 140
33 Event Code 120 142
34 Event Code 121 142
35 Event Code 140 143
36 Event Code 141 143
37 Event Code 142 144
38 Event Code 143 144
39 Event Code 150 145
40 Event Code 151 147
41 Event Code 300 148
42 Event Code 301 148
43 Event Code 302 149
44 Event Code 310 149
45 Event Code 311 150
46 Event Code 312 150
47 Event Code 400 151
48 Event Code 410 151
49 Event Code 411 152
50 Event Code 412 152
51 Event Code 421 153
52 Event Code 423 153
53 Event Code 426 154
54 Event Code 433 154
55 Event Code 440 155
56 Event Code 442 155
57 Event Code 445 156
58 Event Code 453 157

59 Event Code 506 158
60 Event Code 507 159
61 Event Code 508 159
62 Event Code 510 160
63 Event Code 512 160
64 Event Code 513 161
65 Event Code 514 161
66 Event Code 523 162
67 Event Code 524 162
68 Event Code 525 163
69 Event Code 581 163
70 Event Code 582 164
71 Event Code 583 164
72 Event Code 584 165
73 Event Code 585 165
74 Event Code 586 166
75 Event Code 810 167
76 Event Code 811 167

about this guide

This service manual provides information to help you:

- Monitor and troubleshoot the Edge Switch 2/12.
- Perform procedures to isolate and resolve problems.
- Repair and maintain the switch.
- Remove and replace field replaceable units (FRUs).

“About this Guide” topics include:

- Overview, page 10
- Conventions, page 11
- Rack Stability, page 13
- Getting Help, page 14

Overview

This section covers the following topics:

- Intended Audience
- Related Documentation

Intended Audience

This book is intended for use by service technicians who are experienced with the following:

- Fibre Channel technology.
- StorageWorks Fibre Channel switches by Hewlett-Packard.

Related Documentation

For a list of corresponding documentation included with this product, see the Related Documents section of the HP StorageWorks Edge Switch Release Notes.

For the latest information, documentation, and firmware releases, please visit the HP StorageWorks website:

http://h18006.www1.hp.com/storage/saninfrastructure.html

For information about Fibre Channel standards, visit the Fibre Channel Industry Association website, located at http://www.fibrechannel.org/.

Conventions

Conventions consist of the following:

- Document Conventions
- Text Symbols
- Equipment Symbols

Document Conventions

The document conventions included in Table 1 apply in most cases.

Table 1: Document Conventions

Element	Convention
Cross-reference links	Blue text: Figure 1
Key and field names, menu items, buttons, and dialog box titles	**Bold**
File names, application names, and text emphasis	*Italics*
User input, command and directory names, and system responses (output and messages)	`Monospace font` `COMMAND NAMES` are uppercase monospace font unless they are case sensitive
Variables	`<monospace, italic font>`
Website addresses	Blue, underlined sans serif font text: http://www.hp.com

Text Symbols

The following symbols may be found in the text of this guide. They have the following meanings.

WARNING: Text set off in this manner indicates that failure to follow directions in the warning could result in bodily harm or death.

Caution: Text set off in this manner indicates that failure to follow directions could result in damage to equipment or data.

Note: Text set off in this manner presents commentary, sidelights, or interesting points of information.

Equipment Symbols

The following equipment symbols may be found on hardware for which this guide pertains. They have the following meanings.

Any enclosed surface or area of the equipment marked with these symbols indicates the presence of electrical shock hazards. Enclosed area contains no operator serviceable parts.

WARNING: To reduce the risk of personal injury from electrical shock hazards, do not open this enclosure.

Any RJ-45 receptacle marked with these symbols indicates a network interface connection.

WARNING: To reduce the risk of electrical shock, fire, or damage to the equipment, do not plug telephone or telecommunications connectors into this receptacle.

Any surface or area of the equipment marked with these symbols indicates the presence of a hot surface or hot component. Contact with this surface could result in injury.

WARNING: To reduce the risk of personal injury from a hot component, allow the surface to cool before touching.

Power supplies or systems marked with these symbols indicate the presence of multiple sources of power.

WARNING: To reduce the risk of personal injury from electrical shock, remove all power cords to completely disconnect power from the power supplies and systems.

Any product or assembly marked with these symbols indicates that the component exceeds the recommended weight for one individual to handle safely.

WARNING: To reduce the risk of personal injury or damage to the equipment, observe local occupational health and safety requirements and guidelines for manually handling material.

Rack Stability

Rack stability protects personnel and equipment.

WARNING: To reduce the risk of personal injury or damage to the equipment, be sure that:

- The leveling jacks are extended to the floor.
- The full weight of the rack rests on the leveling jacks.
- In single rack installations, the stabilizing feet are attached to the rack.
- In multiple rack installations, the racks are coupled.
- Only one rack component is extended at any time. A rack may become unstable if more than one rack component is extended for any reason.

Getting Help

If you still have a question after reading this guide, contact an HP authorized service provider or access our website: http://www.hp.com.

HP Technical Support

Telephone numbers for worldwide technical support are listed on the following HP website: http://welcome.hp.com/country/us/en/support.html. From this website, select the country of origin.

Note: For continuous quality improvement, calls may be recorded or monitored.

Be sure to have the following information available before calling:

- Technical support registration number (if applicable)
- Product serial numbers
- Product model names and numbers
- Applicable error messages
- Operating system type and revision level
- Detailed, specific questions

HP Storage Website

The HP website has the latest information on this product, as well as the latest drivers. Access storage at: http://welcome.hp.com/country/us/eng/prodserv.html. From this website, select the appropriate product or solution.

HP Authorized Reseller

For the name of your nearest HP authorized reseller:

- In the United States, call 1-800-345-1518
- In Canada, call 1-800-263-5868
- Elsewhere, see the HP website for locations and telephone numbers: http://www.hp.com.

General Information

1

The HP StorageWorks Edge Switch 2/12 provides up to 12 ports of low-cost and high-performance dynamic Fibre Channel connectivity for switched fabric devices or arbitrated loop devices. The switch allows low-cost, low-bandwidth workgroup (edge) devices to communicate with mainframe servers, mass storage devices, or other peripherals, and ultimately be incorporated into an enterprise storage area network (SAN) environment.

This chapter provides the following information:

- Switch Description, page 15
- Error-Detection, Reporting, and Serviceability Features, page 17
- Software Diagnostic Features, page 18
- Maintenance Approach, page 21
- Tools and Test Equipment, page 22
- Additional Information, page 24

Switch Description

The Edge Switch 2/12 provides Fibre Channel device connectivity through 12 ports that operate at either 1.0625 or 2.125 gigabits per second (Gbps), and can be configured as:

- Fabric ports (F_Ports) to provide direct connectivity for up to 12 switched fabric devices.
- Fabric loop ports (FL_Ports) to provide arbitrated loop connectivity and fabric attachment for FC-AL devices. Each FL_Port can theoretically support the connection of 126 FC-AL devices.
- Expansion ports (E_Ports, G_Ports and Gx_Ports) to provide interswitch link (ISL) connectivity to fabric directors and switches. Expansion port connectivity is not standard, and must be configured through the optional E_Port (or Full Fabric) feature key.

The switch can be installed on a table or desk top, or mounted in an equipment cabinet or in any standard equipment rack.

Figure 1 illustrates the switch.

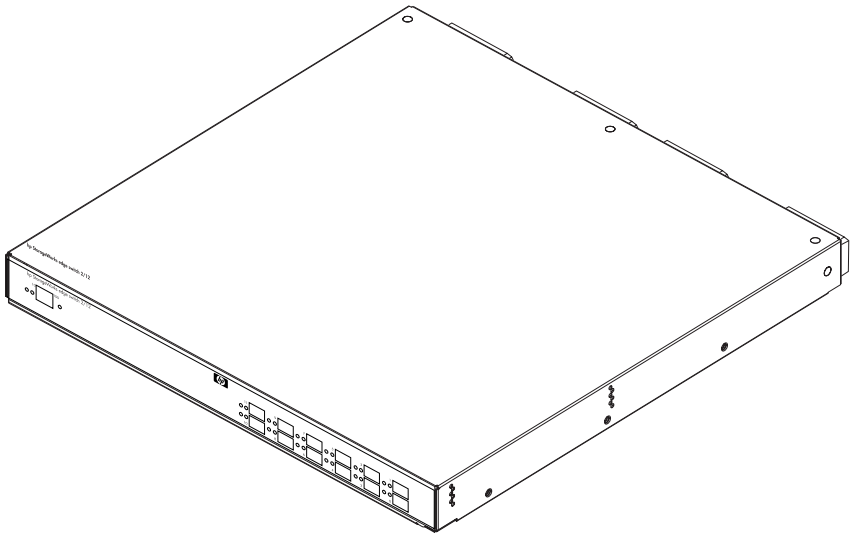

Figure 1: Edge Switch 2/12

Administrators or operators with a browser-capable PC and an Ethernet connection can monitor and manage the switch through the Embedded Web Server (EWS) interface. The EWS interface manages only a single switch, and provides a graphical user interface (GUI) that supports product configuration, statistics monitoring, and basic operation. The EWS interface is opened from a standard Web browser running Netscape Navigator® 4.6 or higher or Microsoft® Internet Explorer 4.0 or higher. At the browser, enter the Internet Protocol (IP) address of the switch as the Internet uniform resource locator (URL). When prompted at a login screen, enter a user name and password.

The Edge Switch 2/12 provides connectivity for devices manufactured by multiple original equipment manufacturers (OEMs). To determine if an OEM product can communicate through connections provided by the switch, or if communication restrictions apply, refer to the supporting publications for the product or contact your HP representative.

Error-Detection, Reporting, and Serviceability Features

The switch provides the following error detection, reporting, and serviceability features:

- LEDs on the switch and adjacent to Fibre Channel ports that provide visual indicators of hardware status or malfunctions.
- FRUs–small form factor pluggable (SFP) optical transceivers–that are removed or replaced without disrupting switch or Fibre Channel link operation.
- A modular design that enables quick removal and replacement of FRUs without the use of tools or equipment.
- System alerts and logs that display switch and Fibre Channel link status at the EWS interface.
- Diagnostic software that performs power-on self-tests (POSTs) and port diagnostics (loopback tests).
- An RS-232 maintenance port at the rear of the switch (port access is password protected) that enables installation or service personnel to change the switch's IP address, subnet mask, and gateway address.

  These parameters can also be changed through a Telnet session, access for which is provided through a local or remote PC with an Ethernet connection to the switch.
- Data collection through the EWS interface to help isolate system problems. The data includes a memory dump file and audit, hardware, and engineering logs.
- Beaconing to assist service personnel in locating a specific port or switch. When port beaconing is enabled, the amber LED associated with the port flashes. When unit beaconing is enabled, the system error indicator on the front panel flashes. Beaconing does not affect port or switch operation.
- SNMP management using the Fibre Channel Fabric Element MIB (Version 1.1), Transmission Control Protocol/Internet Protocol (TCP/IP) MIB-II definition (RFC 1157), or a product-specific private enterprise MIB that runs on the switch. Up to six authorized management workstations can be configured through the EWS interface to receive unsolicited SNMP trap messages. The trap messages indicate product operational state changes and failure conditions.

Software Diagnostic Features

The switch provides the following diagnostic software features that aid in fault isolation and repair of problems:

- SFP transceivers provide on-board diagnostic and monitoring circuits that continuously report status to the EWS interface. The interface provides system alerts and logs that display failure and diagnostic information.
- Unsolicited SNMP trap messages that indicate operational state changes or failures can be transmitted to up to six authorized management workstations.

EWS Interface

The EWS interface provides a GUI accessed through an Ethernet network (locally or remotely) to manage, monitor, and isolate problems for the Edge Switch 2/12. When the interface opens, the default display is the **View** panel, as shown in Figure 2.

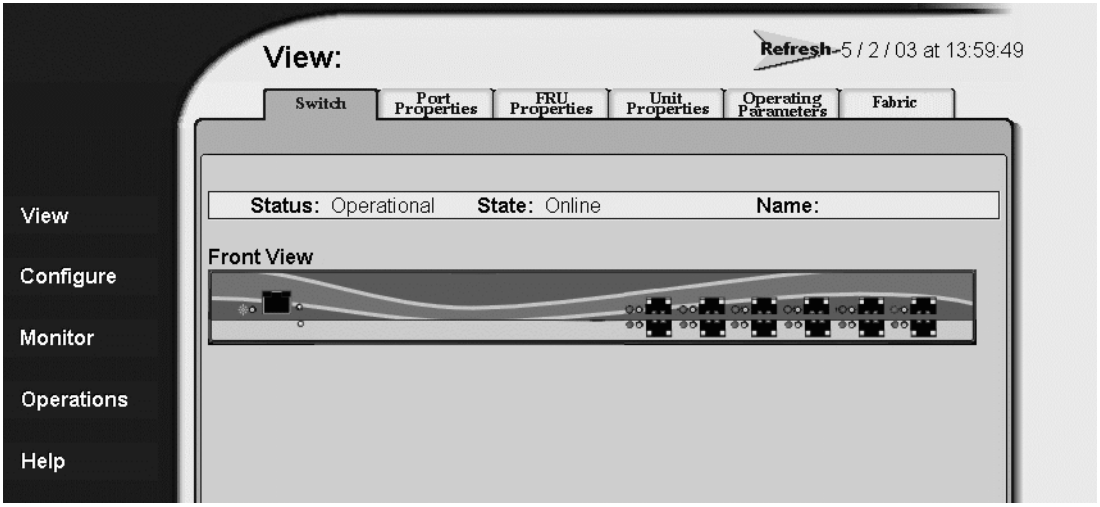

Figure 2: EWS interface: View panel

Task selection tabs appear at the top of the panel, a graphical representation of the switch hardware (front only) appears at the right side of the panel, and menu selections (**View**, **Configure**, **Monitor**, **Operations**, and **Help**) appear at the left side of the panel.

The task selection tabs allow personnel to perform switch-specific tasks, and are a function of the menu selected as follows:

- **View -** At the **View** panel, the **Switch** (default), **Port Properties**, **FRU Properties**, **Unit Properties**, **Operating Parameters**, and **Fabric** task selection tabs appear.
- **Configure -** At the **Configure** panel, the **Ports** (default), **Switch**, **Management**, **Zoning**, **Security**, and **Performance** task selection tabs appear.
- **Monitor -** At the **Monitor** panel, the **Port List** (default), **Port Stats**, **Log**, and **Node List** task selection tabs appear.
- **Operations -** At the **Operations** panel, the **Switch** (default), **Port**, **Maintenance**, and **Feature Installation** task selection tabs appear.
- **Help -** The **Help** selection opens online user documentation that supports the EWS interface.

SNMP Trap Message Support

Unsolicited SNMP trap messages that indicate switch operational state changes or failure conditions can be customer-configured to be transmitted to up to six management workstations. If installed on a dedicated Ethernet LAN, the workstations communicate directly with each switch. If installed on a customer intranet, the workstations communicate with switches through the browser-capable PC.

SNMP data and trap messages are defined in the Fibre Channel FE-MIB definition, a subset of the TCP/IP MIB-II definition (RFC 1157), and a custom, switch-specific MIB. Customers can install these MIBs (in standard ASN.1 format) on any SNMP management workstation.

Although SNMP trap messages are typically transmitted to customer personnel only, the messages may be provided to service personnel as initial notification of a switch problem or as information included in the fault isolation process. Generic SNMP traps include:

- **coldStart -** reports that the SNMP agent is reinitializing due to a switch reset.
- **warmStart -** reports that the SNMP agent is reinitializing due to a switch reset or initial program load (IPL).
- **authorizationFailure -** reports attempted access by an unauthorized SNMP manager. This trap is configurable and is disabled by default.

Switch-specific SNMP traps specified in the custom MIB include Fibre Channel port operational state changes and FRU operational state changes.

If authorized through the EWS interface, users at SNMP management workstations can modify MIB variables. For additional information, refer to the *HP StorageWorks SNMP Reference Guide for Directors and Edge Switches*.

Maintenance Approach

Whenever possible, the maintenance approach instructs service personnel to perform fault isolation and repair procedures without degrading or interrupting operation of the switch, attached devices, or associated applications.

Switch fault isolation begins when one or more of the following occur:

- System event information displays at the EWS interface.
- LEDs on the switch front panel or adjacent to Fibre Channel ports illuminate to indicate a hardware malfunction.
- An unsolicited SNMP trap message is received at a management workstation, indicating an operational state change or failure.

System events can be related to a:

- Switch failure (hardware or software)
- Ethernet LAN communication failure between the switch and a PC accessing the EWS interface
- Link failure between a port and attached device
- ISL failure or segmentation of an E_Port

Fault isolation and service procedures vary depending on the system event information provided. Fault isolation and related service information are provided through maintenance analysis procedures (MAPs) documented in Chapter 3. MAPs consist of step-by-step procedures that prompt service personnel for information or describe a specific action to be performed.

MAPs provide information to interpret system event information, isolate a switch failure to a single FRU, remove and replace the failed FRU, and verify switch operation. The fault isolation process normally begins with “MAP 0000: Start MAP” on page 30.

Before using these procedures, ensure the correct switch is selected for service by enabling unit beaconing at the failed switch. The amber system error (ERR) LED on the switch front panel blinks when beaconing is enabled. Instructions to enable beaconing are incorporated into MAP steps.

Tools and Test Equipment

This section describes tools and test equipment that may be required to install, test, service, and verify operation of the switch.

Tools Supplied with the Switch

Tools are supplied with the switch or must be supplied by service personnel. Use of the tools may be required to perform one or more installation, test, service, or verification tasks.

- Fiber-optic loopback plug - An SFP multi-mode (shortwave laser) or single-mode (longwave laser) loopback plug is required to perform port loopback diagnostic tests. One loopback plug is shipped with the switch, depending on the type of port transceivers installed. Both plugs are shipped if shortwave laser and longwave laser transceivers are installed. The plug is shown in Figure 3.

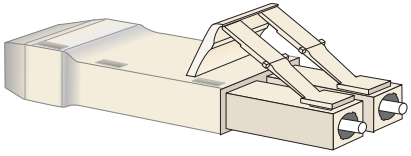

Figure 3: Multi-mode and single-mode loopback plugs

- **Fiber-optic protective plug–**For safety and port transceiver protection, fiber-optic protective plugs must be inserted in all port SFPs without fiber-optic cables attached. The switch is shipped with protective plugs installed in all ports. A protective plug is shown in Figure 4.

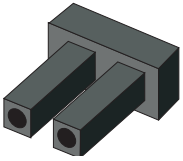

Figure 4: Fiber-optic protective plug

- **Null modem cable–**An asynchronous RS-232 null modem cable is required to configure switch network addresses and acquire event log information through the maintenance port. The cable has nine conductors and DB-9 male and female connectors. A null modem cable is not a standard (straight-through) RS-232 cable. Refer to Figure 5.

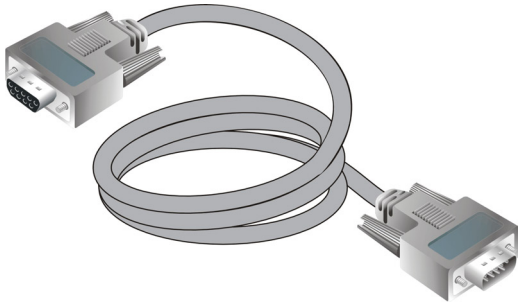

Figure 5: Null modem cable

Tools Supplied by Service Personnel

The following tools are expected to be supplied by service personnel performing switch installation and maintenance actions. Use of the tools may be required to perform one or more installation, test, service, or verification tasks.

- **Scissors or pocket knife–**A sharp cutting edge (scissors or knife blade) may be required to cut the protective strapping when unpacking the switch or replacement FRUs.
- **Standard flat-tip and cross-tip (Phillips) screwdrivers–**Screwdrivers are required to remove, replace, adjust, or tighten various connector or chassis components.
- **Maintenance terminal (desktop or notebook PC)–**The PC is required to configure switch network addresses and acquire event log information through the maintenance port.

  The PC must have:

  — The Microsoft® Windows® 98, Windows 2000, or Windows Millennium Edition operating system installed.

  — RS-232 serial communication software (such as *ProComm Plus*™ or *HyperTerminal*) installed. *HyperTerminal* is provided with Windows operating systems.
- **Fiber-optic cleaning kit–**The kit contains tools and instructions to clean fiber-optic cable, connectors, loopback plugs, and protective plugs.

Additional Information

The following Edge Switch 2/12 documents provide additional information:

- For detailed information about Edge Switch 2/12 front and rear panel features, field replaceable units (FRUs), management options, operational features, optional kits, installation, configuration and technical specifications, refer to the *HP StorageWorks Edge Switch 2/12 Installation Guide*.
- For information on managing the Edge Switch 2/12 using the Embedded Web Server interface, refer to the *HP StorageWorks Embedded Web Server User Guide.*

Diagnostics

2

This chapter describes diagnostic procedures used by service representatives to isolate HP StorageWorks Edge Switch 2/12 problems or failures to the field replaceable unit (FRU) level. The chapter specifically describes how to perform maintenance analysis procedures (MAPs).

Maintenance Analysis Procedures

MAPs provide fault isolation and related service procedures. MAPs consist of step-by-step procedures that prompt service personnel for information or describe a specific action to be performed. MAPs provide information to interpret system events, isolate a switch failure, repair the failure, and verify switch operation.

Factory Defaults

Table 2 lists the defaults for the passwords, and IP, subnet, and gateway addresses for the Edge Switch 2/12.

Table 2: Factory-Set Defaults

Item	Default
Customer password	password
Maintenance password	level-2
IP address	10.1.1.10
Subnet mask	255.0.0.0
Gateway address	0.0.0.0

Quick Start

Table 3 lists and summarizes the MAPs. Fault isolation normally begins at MAP 0000: Start MAP on page 30.

Table 3: MAP Summary

MAP	Page
MAP 0000: Start MAP	page 30
MAP 0100: Power Distribution Analysis	page 41
MAP 0200: POST Failure Analysis	page 44
MAP 0300: Loss of Web Browser PC Communication	page 46
MAP 0400: FRU Failure Analysis	page 52
MAP 0500: Port Failure and Link Incident Analysis	page 57
MAP 0600: Fabric, ISL, and Segmented Port Problem Determination	page 74

Table 4 lists event codes and the corresponding MAP references. The table provides a quick start guide if an event code is readily available.

Table 4: Event Codes versus Maintenance Action

Event Code	Explanation	Action
011	Login Server database invalid.	Go to MAP 0600: Fabric, ISL, and Segmented Port Problem Determination.
021	Name Server database invalid.	Go to MAP 0600: Fabric, ISL, and Segmented Port Problem Determination.
031	SNMP request received from unauthorized community.	Add a community name through the EWS interface.
051	Management Server database invalid.	Go to MAP 0600: Fabric, ISL, and Segmented Port Problem Determination.
052	Management Server internal error.	Go to MAP 0600: Fabric, ISL, and Segmented Port Problem Determination.
061	Fabric Controller database invalid.	Go to MAP 0600: Fabric, ISL, and Segmented Port Problem Determination.

Table 4: Event Codes versus Maintenance Action (Continued)

Event Code	Explanation	Action
062	Maximum interswitch hop count exceeded.	Go to MAP 0600: Fabric, ISL, and Segmented Port Problem Determination.
063	Remote switch has too many ISLs.	Go to MAP 0600: Fabric, ISL, and Segmented Port Problem Determination.
070	E_Port is segmented.	Go to MAP 0600: Fabric, ISL, and Segmented Port Problem Determination.
071	Switch is isolated.	Go to MAP 0600: Fabric, ISL, and Segmented Port Problem Determination.
072	E_Port connected to unsupported switch.	Go to MAP 0600: Fabric, ISL, and Segmented Port Problem Determination.
073	Fabric initialization error.	Go to Collect Maintenance Data on page 102.
074	ISL frame delivery error threshold exceeded.	Go to Collect Maintenance Data on page 102.
080	Unauthorized worldwide name.	Go to MAP 0500: Port Failure and Link Incident Analysis.
081	Invalid attachment.	Go to MAP 0500: Port Failure and Link Incident Analysis
120	Error detected while processing system management command.	Go to Collect Maintenance Data on page 102.
121	Zone set activation failed - zone set too large.	Reduce size of zone set and retry.
140	Congestion detected on an ISL.	Go to MAP 0600: Fabric, ISL, and Segmented Port Problem Determination.
141	Congestion relieved on an ISL.	No action required.
142	Low BB_Credit detected on an ISL.	Go to MAP 0600: Fabric, ISL, and Segmented Port Problem Determination.
143	Low BB_Credit relieved on an ISL.	No action required.

Table 4: Event Codes versus Maintenance Action (Continued)

Event Code	Explanation	Action
150	Zone merge failure.	Go to MAP 0600: Fabric, ISL, and Segmented Port Problem Determination.
151	Fabric configuration failure.	Go to Collect Maintenance Data on page 102.
300	Cooling fan propeller failed.	Go to MAP 0400: FRU Failure Analysis.
301	Cooling fan propeller failed.	Go to MAP 0400: FRU Failure Analysis.
302	Cooling fan propeller failed.	Go to MAP 0400: FRU Failure Analysis.
310	Cooling fan propeller recovered.	No action required.
311	Cooling fan propeller recovered.	No action required.
312	Cooling fan propeller recovered.	No action required.
400	Power-up diagnostic failure.	Go to MAP 0200: POST Failure Analysis.
410	Switch reset.	No action required.
411	Firmware fault.	Go to MAP 0200: POST Failure Analysis.
412	CTP watchdog timer reset.	Go to Collect Maintenance Data on page 102.
421	Firmware download complete.	No action required.
423	CTP firmware download initiated.	No action required.
426	Multiple ECC single-bit errors occurred.	Go to MAP 0400: FRU Failure Analysis.
433	Non-recoverable Ethernet fault.	Go to MAP 0400: FRU Failure Analysis.
440	Embedded port hardware failed.	Go to MAP 0400: FRU Failure Analysis.
442	Embedded port anomaly detected.	No action required.
445	ASIC detected a system anomaly.	No action required.
453	New feature key installed.	No action required.

Table 4: Event Codes versus Maintenance Action (Continued)

Event Code	Explanation	Action
506	Fibre Channel port failure.	Go to MAP 0500: Port Failure and Link Incident Analysis.
507	Loopback diagnostics port failure.	Go to MAP 0500: Port Failure and Link Incident Analysis.
508	Fibre Channel port anomaly detected.	No action required.
510	SFP optical transceiver hot-insertion initiated.	No action required.
512	SFP optical transceiver nonfatal error.	Go to MAP 0500: Port Failure and Link Incident Analysis.
513	SFP optical transceiver hot-removal completed.	No action required.
514	SFP optical transceiver failure.	Go to MAP 0500: Port Failure and Link Incident Analysis.
523	FL_Port open request failed.	No action required.
524	No AL_PA acquired.	No action required.
525	FL_Port arbitration timeout.	No action required.
581	Implicit incident.	Go to MAP 0500: Port Failure and Link Incident Analysis.
582	Bit error threshold exceeded.	Go to MAP 0500: Port Failure and Link Incident Analysis.
583	Loss of signal or loss of synchronization.	Go to MAP 0500: Port Failure and Link Incident Analysis.
584	Not operational primitive sequence received.	Go to MAP 0500: Port Failure and Link Incident Analysis.
585	Primitive sequence timeout.	Go to MAP 0500: Port Failure and Link Incident Analysis.
586	Invalid primitive sequence received for current link state.	Go to MAP 0500: Port Failure and Link Incident Analysis.
810	High temperature warning (CTP thermal sensor).	Go to MAP 0400: FRU Failure Analysis.
811	Critically hot temperature warning (CTP thermal sensor).	Go to MAP 0400: FRU Failure Analysis.

MAP 0000: Start MAP

This MAP describes initial fault isolation for the Edge Switch 2/12. Fault isolation begins at the Web browser PC accessing the EWS interface, failed switch, or switch-attached host.

1

Prior to fault isolation, acquire the following from the customer:

- A system configuration drawing or planning worksheet that includes the customer-supplied Web browser PC accessing the EWS interface, switch, other HP products, and device connections.
- The location of the Web browser PC and all switches.
- The internet protocol (IP) address, gateway address, and subnet mask for the switch reporting the problem.
- The administrator user name and password of the customer- supplied server accessing the EWS interface. Both are case sensitive and required when prompted at the username and password entry dialog box.

Continue to the next step.

2

Are you at a PC with a Web browser (such as Netscape Navigator or Microsoft Internet Explorer), an Ethernet connection to the switch reporting the problem, and communicating with the switch through the EWS interface?

YES	NO
↓	Go to step 19.

3

Is the Web browser PC powered on and communicating with the switch through the Ethernet connection and EWS interface?

NO	YES
↓	Go to step 5.

4

Boot the Web browser PC.

1. Power on the PC in accordance with the instructions delivered with the PC. The Windows desktop appears.
2. Launch the PC browser application by double-clicking the Netscape Navigator or Internet Explorer icon at the Windows desktop.
3. At the **Netsite** field (Netscape Navigator) or **Address** field (Internet Explorer), type `http://xxx.xxx.xxx.xxx`, where *xxx.xxx.xxx.xxx* is the IP address of the switch (obtained in step 1). A username and password entry dialog box appears.
4. Type the user name and password obtained in step 1 and click **OK**. The EWS interface opens with the **View** panel displayed (Figure 6).

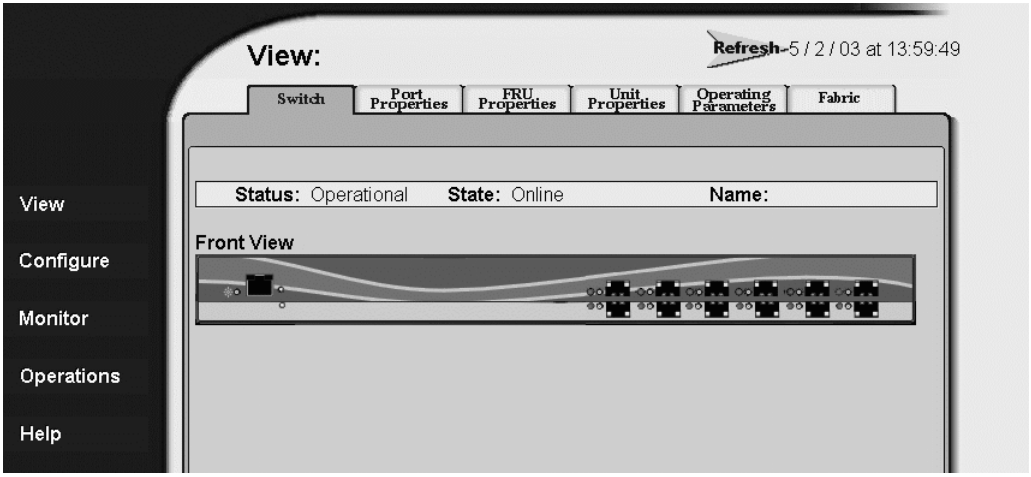

Figure 6: View panel (EWS interface)

Continue to the next step.

5

Does the EWS interface appear operational with the **View** panel displayed?

NO YES

↓ Go to step 10.

6

A `Page cannot be found`, `Unable to locate the server`, `HTTP 404 - file not found`, or other similar message appears. The message indicates the PC cannot communicate with the switch because:

- The switch-to-PC Ethernet link could not be established.
- AC power distribution in the switch failed, or AC power was disconnected.
- The switch control processor (CTP) card failed.

Continue to the next step.

7

Ensure the switch reporting the problem is connected to facility AC power. Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated **PWR** LED (green) or **ERR** LED (amber).
- Illuminated LEDs adjacent to Fibre Channel ports.
- Audio emanations and airflow from cooling fans.

Does the switch appear powered on?

YES	NO
↓	A power distribution problem is indicated. Go to "MAP 0100: Power Distribution Analysis" on page 41. Exit MAP.

8

At the front of the switch, inspect the amber **ERR** LED.

Is the LED illuminated?

NO	YES
↓	A FRU failure or link incident is indicated. Go to step 18 to obtain event codes that identify the problem. Exit MAP.

9

A switch-to-PC Ethernet link problem (Ethernet too busy or IP address typed incorrectly) is indicated.

1. Wait approximately five minutes, then attempt to login to the switch again.
2. At the **Netsite** field (Netscape Navigator) or **Address** field (Internet Explorer), type `http://xxx.xxx.xxx.xxx`, where *xxx.xxx.xxx.xxx* is the IP address of the switch (obtained in step 1). A username and password entry dialog box appears.
3. Type the user name and password obtained in step 1 and click **OK**. If the **View** panel does not display, wait another five minutes and perform this step again.

Does the EWS interface appear operational with the **View** panel displayed?

YES	NO
↓	Perform fault isolation at the switch. Go to step 19.

10

At the **View** panel and **Switch** page, inspect the **Status** field at the top of the page.

Does the switch status indicate **Operational**?

NO	YES
↓	The switch appears operational. Exit MAP.

11

Inspect Fibre Channel port operational states.

1. At the **View** panel, click the **Port Properties** tab. The **Port Properties** page displays with port **0** displayed (Figure 7).

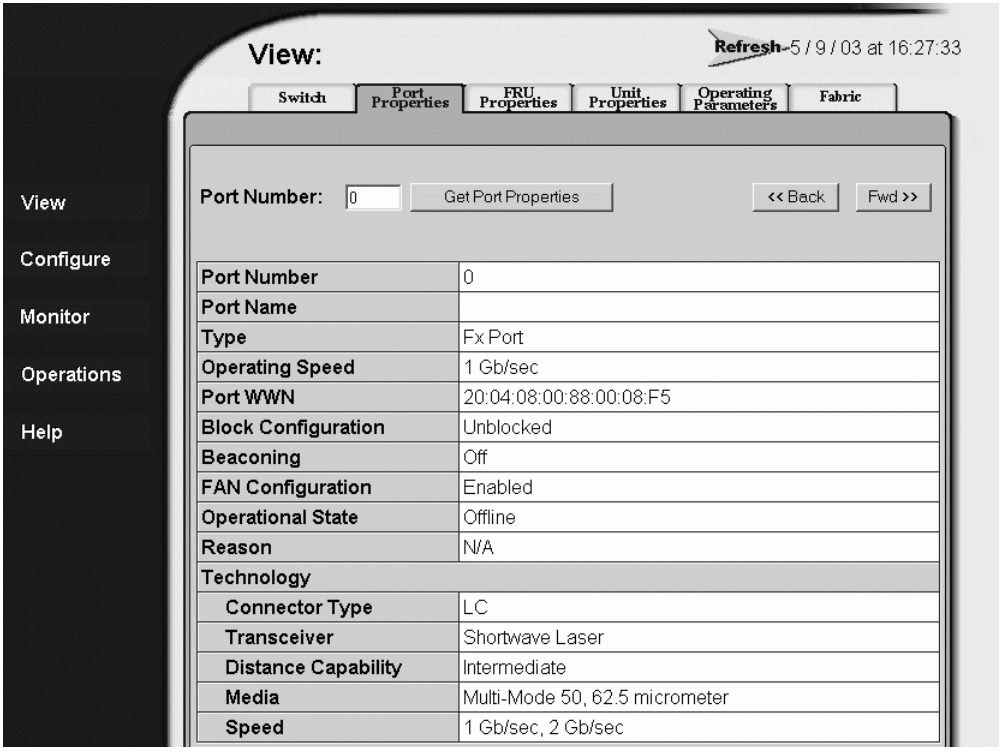

Figure 7: View panel (Port Properties tab)

2. Inspect the **Beaconing** and **Operational State** fields.

Does the **Beaconing** field display an `On` message?

YES NO

↓ Go to step 13.

12

Port beaconing is enabled.

1. Consult the customer and next level of support to determine the reason port beaconing is enabled.

2. Disable port beaconing at the EWS interface:
   a. At the **View** panel, select **Operations** at the left side of the panel. The **Operations** panel opens with the **Switch** and **Beacon** pages displayed.
   b. Click the **Port** tab. The **Operations** panel opens with the **Port** and **Beacon** pages displayed.
   c. Click the check box (checked) in the **Beaconing State** column and click **Activate** to remove the check mark and disable beaconing. The message `Your changes have been successfully activated` appears.

Continue to the next step.

13

At the **View** panel, does the **Operational State** field display a `Segmented` message?

NO YES

↓ Port segmentation is indicated. Go to step 18 to obtain event codes. If no event codes are found, go to "MAP 0600: Fabric, ISL, and Segmented Port Problem Determination" on page 74. Exit MAP.

14

At the **View** panel, does the **Operational State** field display a message indicating a port problem?

NO YES

↓ Go to step 18 to obtain event codes. If no event codes are found, go to "MAP 0500: Port Failure and Link Incident Analysis" on page 57. Exit MAP.

15

Repeat step 11 through step 14 for each remaining Fibre Channel port for which a problem is suspected (ports **0** through **11**).

Is a problem indicated for any of the ports?

NO YES

↓ Go to step 18 to obtain event codes. If no event codes are found, go to "MAP 0500: Port Failure and Link Incident Analysis" on page 57. Exit MAP.

16

Inspect the power supply operational state.

1. At the **View** panel, click the **FRU Properties** tab. The **FRU Properties** page displays (Figure 8).

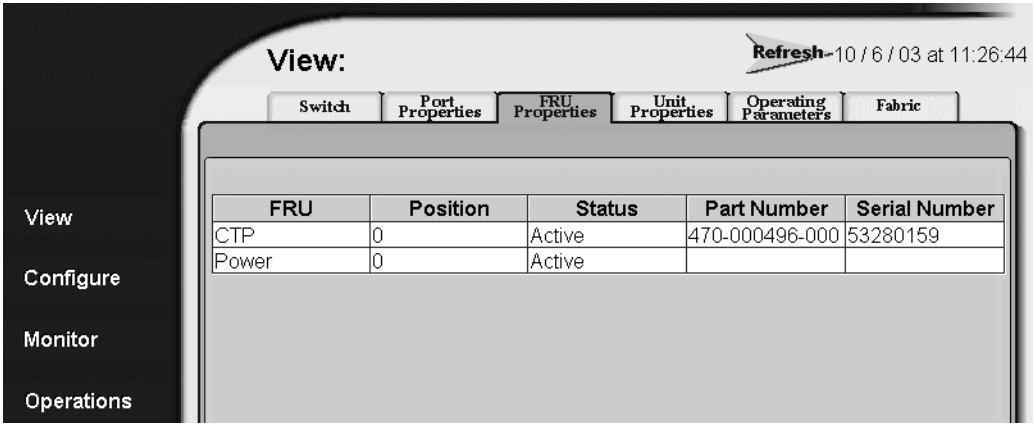

Figure 8: View panel (FRU Properties tab)

2. Inspect the **Status** field for the power supply.

Does the **Status** field display a `Failed` message for the power supply?

NO YES

↓ A power supply failure is indicated. Go to step 18 to obtain event codes. If no event codes are found, go to "MAP 0100: Power Distribution Analysis" on page 41. Exit MAP.

17

Inspect the **Status** fields for switch FRUs.

Does the **State** field display a **Failed** message for any of the FRUs?

YES NO

↓ The switch appears operational. Exit MAP.

A FRU failure is indicated. Continue to the next step to obtain event codes. If no event codes are found, go to "MAP 0400: FRU Failure Analysis" on page 52. Exit MAP.

18

Obtain event codes from the EWS Event Log.

Note: If multiple event codes are found, note all codes and associated severity levels. Record the date, time, and listed sequence, and determine if the codes are related to the reported problem. Begin fault isolation with the most recent event code with the highest severity level. Other codes may accompany this event code, or may indicate a normal indication after a problem is resolved.

1. At the **View** panel, select **Monitor** at the left side of the panel. The **Monitor** panel opens with the **Port List** page displayed.
2. Click the **Log** tab. The **Log** page displays (Figure 9).

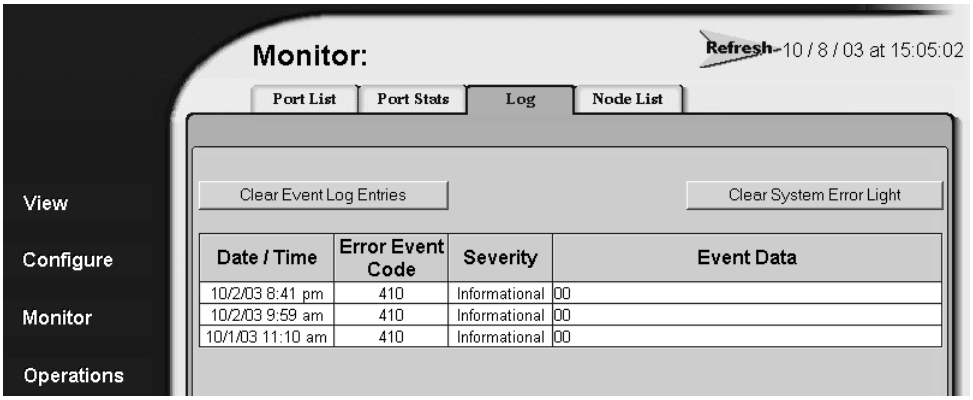

Figure 9: Monitor panel (Log page)

3. Record the event code, date, time, and severity (Informational, Minor, Major, or Severe).
4. Record all event codes that may relate to the reported problem.

Were one or more event codes found?

NO YES

↓ Go to Table 4 on page 26 to interpret event codes. Exit MAP.

Return to step 1 and perform fault isolation again. If this is the second time at this step, contact the next level of support. Exit MAP.

19

At the switch, is the green PWR LED at the switch front bezel illuminated?

NO YES

↓ Go to step 24.

20

Is the switch connected to facility AC power?

NO YES

↓ Go to step 23.

21

Connect the switch to facility AC power. Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated **PWR** LED (green) or **ERR** LED (amber).
- Illuminated LEDs adjacent to Fibre Channel ports.
- Audio emanations and airflow from cooling fans.

Does the switch appear powered on?

YES NO

↓ A power distribution problem is indicated. Go to step 18 to obtain event codes. If no event codes are found, go to "MAP 0100: Power Distribution Analysis" on page 41. Exit MAP.

22

Is the green **PWR** LED at the switch front bezel illuminated?

NO **YES**

↓ Go to step 24.

A faulty **PWR** LED is indicated, but switch and Fibre Channel port operation is not disrupted. The LED is connected to CTP card circuitry, and if this problem is a concern to the customer, the switch must be replaced. Exit MAP.

23

Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated **PWR** LED (green) or **ERR** LED (amber).
- Illuminated LEDs adjacent to Fibre Channel ports.
- Audio emanations and airflow from cooling fans.

Does the switch appear powered on?

YES	NO
↓	A power distribution problem is indicated. Go to step 18 to obtain event codes. If no event codes are found, go to "MAP 0100: Power Distribution Analysis" on page 41. Exit MAP.

A faulty **PWR** LED is indicated, but switch and Fibre Channel port operation is not disrupted. The LED is connected to CTP card circuitry, and if this problem is a concern to the customer, the switch must be replaced. Exit MAP.

24

Is the amber **ERR** LED at the switch front bezel blinking?

YES	NO
↓	Go to step 26.

25

Unit beaconing is enabled for the switch.

1. Consult the customer and next level of support to determine the reason unit beaconing is enabled.
2. Disable unit beaconing at the EWS interface.
   a. At the **View** panel, select **Operations** at the left side of the panel. The **Operations** panel opens with the **Switch** and **Beacon** pages displayed.
   b. Click **Deactivate** to disable beaconing. The message `Your changes have been successfully activated` appears.

Was unit beaconing enabled because switch failure or degradation was suspected?

YES	NO
↓	The switch appears operational. Exit MAP.

Go to step 19 and perform fault isolation again (at the switch). If this is the second time at this step, contact the next level of support. Exit MAP.

26

Is the amber **ERR** LED at the switch front bezel illuminated?

YES	NO
↓	The switch appears operational. Exit MAP.

27

Check FRUs for failure symptoms.

Are any amber LEDs associated with Fibre Channel ports illuminated?

NO	YES
↓	A Fibre Channel port failure is indicated. Go to step 18 to obtain event codes. If no event codes are found, go to "MAP 0500: Port Failure and Link Incident Analysis" on page 57. Exit MAP.

A link incident is indicated. Go to step 18 to obtain event codes. If no event codes are found, go to "MAP 0500: Port Failure and Link Incident Analysis" on page 57. Exit MAP.

28

The link incident record provides the attached switch port number(s) and one or more of the following event codes and messages. Record all event codes that may relate to the reported problem.

581 - Link interface incident - implicit incident.

582 - Link interface incident - bit-error threshold exceeded.

583 - Link failure - loss of signal or loss of synchronization.

584 - Link failure - not-operational primitive sequence received.

585 - Link failure - primitive sequence timeout.

586 - Link failure - invalid primitive sequence received for the current link state.

Were one or more event codes found?

YES	NO
↓	Perform fault isolation at the switch. Go to step 19.

Go to Table 4 on page 26 to interpret event codes. Exit MAP.

MAP 0100: Power Distribution Analysis

This MAP describes fault isolation for the switch power distribution system, including a defective AC power cord or power supply.

1

Is fault isolation being performed at the switch?

YES	NO
↓	Fault isolation is being performed at the EWS interface. Go to step 8.

2

Verify the switch is connected to facility power and is powered on.

1. Ensure the AC power cord is connected to the rear of the switch and a facility power receptacle. If not, connect the cord as directed by the customer.
2. Ensure the associated facility circuit breaker is on. If not, ask the customer to set the circuit breaker on.
3. Ensure the AC power cord is not damaged. If damaged, replace the cord.

Was a corrective action performed?

YES	NO
↓	Go to step 4.

3

Verify power supply and switch operation. Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated **PWR** LED (green) or **ERR** LED (amber).
- Illuminated LEDs adjacent to Fibre Channel ports.
- Audio emanations and airflow from cooling fans.

Is a power supply or power distribution system failure indicated?

YES	NO
↓	The switch appears operational. Exit MAP.

4

Have the customer inspect and verify that facility power is within specifications. These specifications are:

- One single-phase connection for the power supply.
- Input power between 100 and 240 VAC, and at least 5 amps.
- Input frequency between 47 and 63 Hz.

Is facility power within specifications?

YES	NO
↓	Ask the customer to correct the facility power problem. When facility power is corrected, continue to the next step.

5

Verify power supply and switch operation. Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated **PWR** LED (green) or **ERR** LED (amber).
- Illuminated LEDs adjacent to Fibre Channel ports.
- Audio emanations and airflow from cooling fans.

Is a power supply or power distribution system failure indicated?

YES	NO
↓	The switch appears operational. Exit MAP.

6

The power supply may be operational, but the CTP card is not receiving DC power. The in-card circuit breaker may have tripped due to a power surge, or the CTP card failed. Disconnect the power cord, then reconnect the cord (power cycle the switch) to reset the CTP card.

Did power cycling the switch solve the problem?

NO	YES
↓	The switch appears operational. Exit MAP.

7

Visual inspection indicates a power supply, power distribution system, or CTP card failure. Replace the switch. Exit MAP.

8

Does the EWS interface appear operational?

NO	YES
↓	Go to step 11.

9

A `Page cannot be found`, `Unable to locate the server`, `HTTP 404 - file not found`, or other similar message appears. The message indicates the PC cannot communicate with the switch because:

- The switch-to-PC Ethernet link could not be established.
- AC power distribution in the switch failed, or AC power was disconnected.
- The switch CTP card failed.

Continue to the next step.

10

Ensure the switch reporting the problem is connected to facility AC power. Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated **PWR** LED (green) or **ERR** LED (amber).
- Illuminated LEDs adjacent to Fibre Channel ports.
- Audio emanations and airflow from cooling fans.

Is a power supply or power distribution system failure indicated?

YES	NO
↓	Analysis for an Ethernet link or CTP card failure is not described in this MAP. Go to "MAP 0000: Start MAP" on page 30. If this is the second time at this step, contact the next level of support. Exit MAP.

11

Inspect the power supply operational state at the EWS interface.

1. At the **View** panel, click the **FRU Properties** tab. The **FRU Properties** tab displays.
2. Inspect the **Status** field for the power supply.

Does the **Status** field display a `Failed` message for the power supply?

NO YES

↓ The power supply failed. Replace the switch. Exit MAP.

The switch appears operational. Exit MAP.

MAP 0200: POST Failure Analysis

When the switch is powered on, it performs a series of power-on self-tests (POSTs). When POSTs complete, the switch performs an initial machine load (IML) that loads firmware and brings the unit online. This MAP describes fault isolation for problems that may occur during the POST/IML process.

If an error occurs, the POST/IML process continues in an attempt to initialize the switch and bring it online. An event code **400** displays when the switch completes the POST/IML process.

1

Ensure the switch reporting the problem is connected to facility AC power. Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated **PWR** LED (green) or **ERR** LED (amber).
- Illuminated LEDs adjacent to Fibre Channel ports.
- Audio emanations and airflow from cooling fans.

Does the switch appear powered on?

YES NO

↓ An AC power distribution problem is indicated, and analysis for the failure is not described in this MAP. Go to "MAP 0100: Power Distribution Analysis" on page 41. Exit MAP.

2

Was an event code **400** or **411** observed at the EWS Event Log?

YES NO

↓ Analysis for the failure is not described in this MAP. Go to "MAP 0000: Start MAP" on page 30. Exit MAP.

3

Table 5 lists event codes, brief explanations of the codes, and the suggested actions to isolate faults.

Table 5: MAP 0200 Event Codes

Event Code	Explanation	Action
400	Power-up diagnostic failure.	Go to step 4.
411	Firmware fault.	Go to step 8.

4

POST/IML diagnostics detected a FRU failure as indicated by event code **400** with supplementary event data.

1. At the EWS Event Log, examine the first two bytes (**0** and **1**) of event data associated with event code **400**.
2. Byte **0** is a FRU code that indicates the failed FRU. Byte **1** is the slot number of the failed FRU (**00** for a nonredundant FRU).

Table 6 lists byte **0** FRU codes and suggested actions to isolate faults.

Table 6: MAP 0200 Byte 0 FRU Codes

Byte 0	Failed FRU	Action
02	CTP card.	Go to step 5.
05	Fan module.	Go to step 6.
06	Power supply.	Go to step 7.

5

The CTP card failed POSTs as indicated by FRU code **02**. Replace the switch. Exit MAP.

6

A cooling fan failed POSTs as indicated by FRU code **05**. Replace the switch. Exit MAP.

7

The power supply failed POSTs as indicated by FRU code **06**. Replace the switch. Exit MAP.

8

POST/IML diagnostics detected a firmware failure, as indicated by event code **411**, and performed an online dump. All Fibre Channel ports reset after the failure and devices momentarily logout, login, and resume operation.

Perform the procedure described in "Collect Maintenance Data" on page 102. Exit MAP.

MAP 0300: Loss of Web Browser PC Communication

This MAP describes fault isolation of the Ethernet communication link between a switch and a web browser PC running the EWS interface. The failure indication is a `Page cannot be found`, `Unable to locate the server`, `HTTP 404 - file not found`, or other similar message.

Caution: Prior to servicing a switch, determine the Ethernet LAN configuration. Installation of multiple switches on a public customer intranet can complicate problem determination and fault isolation.

1

Does the EWS interface appear operational?

NO	YES
↓	The switch-to-EWS PC connection is restored and appears operational. The cause may be an Ethernet adapter reset (on the switch CTP card) in response to an error. The connection to the Web browser PC terminates briefly, then recovers upon reset.

If this intermittent problem continues, perform the procedure described in "Collect Maintenance Data" on page 102. Exit MAP.

2

A `Page cannot be found`, `Unable to locate the server`, `HTTP 404 - file not found`, or other similar message appears. The message indicates the PC cannot communicate with the switch because:

- The switch-to-PC Ethernet link could not be established.
- AC power distribution in the switch failed, or AC power was disconnected.
- The switch CTP card failed.

Continue to the next step.

3

Ensure the switch reporting the problem is connected to facility AC power. Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated **PWR** LED (green) or **ERR** LED (amber).
- Illuminated LEDs adjacent to Fibre Channel ports.
- Audio emanations and airflow from cooling fans.

Does the switch appear powered on?

YES	NO
↓	A power distribution problem is indicated. Go to "MAP 0100: Power Distribution Analysis" on page 41. Exit MAP.

4

At the front of the switch, inspect the amber **ERR** LED.

Is the LED illuminated?

NO	YES
↓	A FRU failure or link incident is indicated. Go to "MAP 0000: Start MAP" on page 30. Exit MAP.

5

Either a switch-to-PC Ethernet link problem (Ethernet too busy or IP address typed incorrectly) or a switch Ethernet port failure is indicated.

1. Wait approximately five minutes, then attempt to login to the switch again.

2. At the **Netsite** field (Netscape Navigator) or **Address** field (Internet Explorer), type `http://xxx.xxx.xxx.xxx`, where *xxx.xxx.xxx.xxx* is the IP address of the switch (obtained in "MAP 0000: Start MAP" on page 30). A username and password entry dialog box appears.
3. Type the user name and password obtained in "MAP 0000: Start MAP" on page 30, and click **OK**. If the **View** panel does not display, wait five minutes and perform this step again.

Does the EWS interface appear operational with the **View** panel displayed?

NO	YES
↓	The switch-to-EWS PC connection is restored and appears operational. Exit MAP.

6

A problem with another LAN-attached device may be indicated.

- If the problem is associated with another switch or server, go to "MAP 0000: Start MAP" on page 30 to isolate the problem for that device. Exit MAP.
- If the problem is associated with an unrelated device, notify the customer and have the system administrator correct the problem.

Did repair of an unrelated LAN-attached device solve the problem?

NO	YES
↓	The switch-to-EWS PC connection is restored and appears operational. Exit MAP.

7

The IP address defining the switch to the Ethernet LAN must be verified. A maintenance terminal (PC) and asynchronous RS-232 null modem cable are required to verify the switch IP address. The tools are provided with the switch or by service personnel. To verify the IP address:

1. Remove the protective cap from the 9-pin maintenance port at the rear of the switch (a phillips-tip screwdriver may be required). Connect the RS-232 null modem cable to the port.
2. Connect the other cable end to a 9-pin communication port (**COM1** or **COM2**) at the rear of the maintenance terminal PC.
3. Power on the maintenance terminal. After the PC powers on, the Windows desktop displays.

4. At the Windows desktop, click **Start** at the left side of the task bar. The **Windows Workstation** menu displays.

Note: The following steps describe inspecting the IP address using HyperTerminal serial communication software.

---

5. At the **Windows Workstation** menu, sequentially select **Programs**, **Accessories**, **Communications**, and **HyperTerminal**. The **Connection Description** dialog box displays (Figure 10).

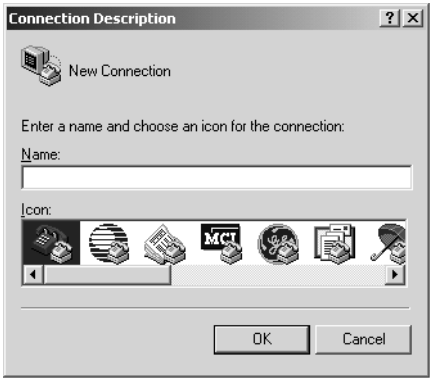

Figure 10: Connection Description dialog box

6. Type `Edge-12` in the **Name** field and click **OK**. The **Connect To** dialog box displays (Figure 11).

Figure 11: Connect To dialog box

7. Ensure the **Connect using** field displays **COM1** or **COM2** (depending on the serial communication port connection to the switch), and click **OK**. The **COMn** dialog box displays, where **n** is **1** or **2** (Figure 12).

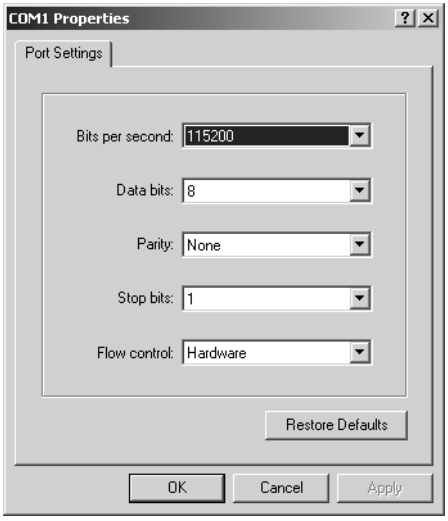

Figure 12: COM*n* Properties dialog box

8. Configure the **Port Settings** parameters as follows:
   - **Bits per second** - 115200.
   - **Data bits** - 8.
   - **Parity** - None.
   - **Stop bits** - 1.
   - **Flow control** - Hardware or None.

   When the parameters are set, click **Apply** and **OK**. The **Edge-12 - HyperTerminal** dialog box displays.
9. At the > prompt, type the user-level password (default is **password**) and press **Enter**. The password is case sensitive. The **Edge-12 - HyperTerminal** dialog box displays with a `C>` prompt at the bottom of the window.
10. At the `C>` prompt, type `ipconfig` and press **Enter**. The **Edge-12 - HyperTerminal** dialog box displays with configuration information listed, including the IP address (Figure 13).

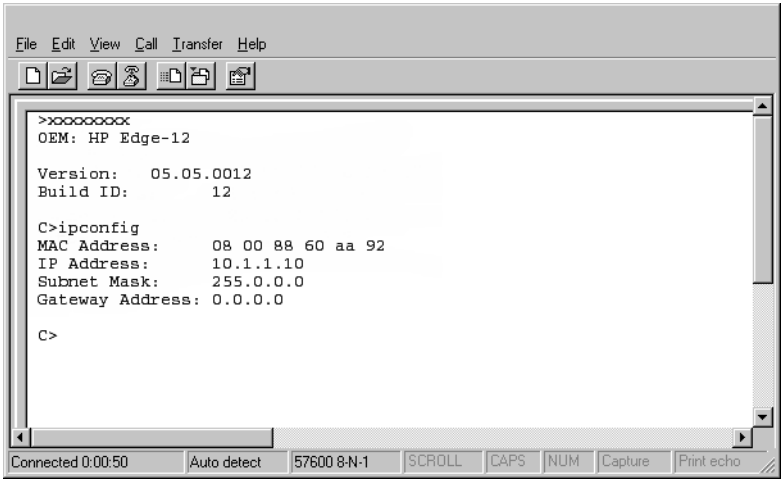

Figure 13: Edge-12 - HyperTerminal dialog box

11. Record the switch IP address.
12. Select **Exit** from the **File** pull-down menu to close the HyperTerminal application. A confirmation message displays (Figure 14).

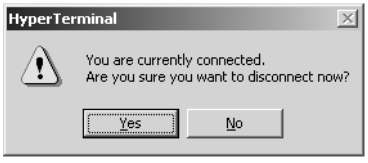

Figure 14: Disconnect message box

13. Click **Yes**. A second **HyperTerminal** dialog box displays (Figure 15).

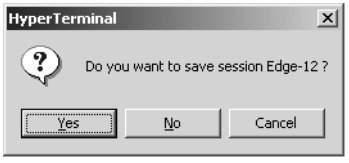

Figure 15: Save Session message box

14. Click **No** to exit and close the HyperTerminal application.
15. Power off the maintenance terminal.

16. Disconnect the RS-232 null modem cable from the switch and the maintenance terminal. Replace the protective cap over the maintenance port.

Did changing the IP address of the switch solve the problem?

NO	YES
↓	The switch-to-EWS PC connection is restored and appears operational. Exit MAP.

Failure of the switch Ethernet port is indicated. Replace the switch. Exit MAP.

MAP 0400: FRU Failure Analysis

This MAP describes fault isolation for the switch and FRUs. Failure indicators include:

- An event code recorded at the EWS Event Log.
- The amber LED on the FRU illuminates.
- A `Failed` message associated with a FRU at the EWS interface.

1

Was an event code **300**, **301**, **302**, **426**, **433**, **440**, **810**, or **811** observed at the EWS **Event Log**?

YES	NO
↓	Go to step 3.

2

Table 7 lists event codes, brief explanations of the codes, and suggested actions to isolate faults.

Table 7: MAP 400 Event Codes

Event Code	Explanation	Action
300	Cooling fan propeller failed.	Go to step 6.
301	Cooling fan propeller failed.	Go to step 6.
302	Cooling fan propeller failed.	Go to step 6.
426	Multiple ECC single-bit errors occurred.	Go to step 10.
433	Non-recoverable Ethernet fault.	Go to step 11.

Table 7: MAP 400 Event Codes (Continued)

Event Code	Explanation	Action
440	Embedded port hardware failed.	Go to step 11.
810	High temperature warning (CTP thermal sensor).	Go to step 10.
811	Critically hot temperature warning (CTP thermal sensor).	Go to step 10.

3

Is fault isolation being performed at the switch?

YES NO

↓ Fault isolation is being performed at the EWS interface. Go to step 12.

4

Ensure the switch reporting the problem is connected to facility AC power. Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated **PWR** LED (green) or **ERR** LED (amber).
- Illuminated LEDs adjacent to Fibre Channel ports.
- Audio emanations and airflow from cooling fans.

Does the switch appear powered on?

YES NO

↓ An AC power distribution or CTP card failure is indicated. Go to "MAP 0000: Start MAP" on page 30. If this is the second time at this step, replace the switch. Exit MAP.

5

Inspect cooling fans at the rear of the switch to ensure all fan blades are rotating.

Does cooling fan inspection indicate a failure (one or more cooling fans not rotating)?

YES NO

↓ Go to step 7.

6

Visual inspection or an event code **300**, **301**, or **302** indicates one or more cooling fans failed. Replace the switch. Exit MAP.

7

Inspect the switch front panel.

Is the green **PWR** LED illuminated and the amber **ERR** LED illuminated and blinking (beaconing)?

YES NO

↓ Go to step 9.

8

Unit beaconing is enabled for the switch.

1. Consult the customer and next level of support to determine the reason unit beaconing is enabled.
2. Disable unit beaconing at the EWS interface.
   a. At the **View** panel, select **Operations** at the left side of the panel. The **Operations** panel opens with the **Switch** and **Beacon** pages displayed.
   b. Click **Deactivate** to disable beaconing. The message `Your changes have been successfully activated` appears.

Was unit beaconing enabled because a failure or degradation was suspected?

NO YES

↓ Go to step 1.

The switch appears operational. Exit MAP.

9

Is the green **PWR** LED illuminated, the amber **ERR** LED illuminated, and all Fibre Channel traffic disrupted (not operational)?

NO YES

↓ A CTP card failure is indicated. Replace the switch. Exit MAP.

Analysis for this failure is not described in this MAP. Go to "MAP 0000: Start MAP" on page 30. If this is the second time at this step, contact the next level of support. Exit MAP.

10

An event code **426** (SDRAM problem), **810** (high-temperature warning), or **811** (critically-hot temperature warning) indicates an intermittent problem that may result in switch failure.

Is the appearance of this event code a recurring problem?

NO	YES
↓	A CTP card failure is indicated. Replace the switch. Exit MAP.

Perform the data collection procedure and contact the next level of support. Refer to "Collect Maintenance Data" on page 102. Exit MAP.

11

An event code **433** or **440** indicates a CTP card failure. Replace the switch. Exit MAP.

12

Does the EWS interface appear operational?

NO	YES
↓	Go to step 14.

13

A `Page cannot be found`, `Unable to locate the server`, `HTTP 404 - file not found`, or other similar message appears. The message indicates the PC cannot communicate with the switch because:

- The switch-to-PC Ethernet link could not be established.
- AC power distribution in the switch failed, or AC power was disconnected.
- The switch CTP card failed.

The EWS interface is not operational and fault isolation must be performed at the switch. Go to step 4.

14

Inspect the power supply (includes fan modules) operational state at the EWS interface.

1. At the **View** panel, click the **FRU Properties** tab. The **FRU Properties** tab displays.
2. Inspect the **Status** field for the power supply.

Does the **Status** field display a `Failed` message for the power supply?

NO	YES
↓	A fan module or power supply failure is indicated. Replace the switch. Exit MAP.

15

Inspect the CTP card operational state at the EWS interface.

1. At the **View** panel, click the **FRU Properties** tab. The **FRU Properties** tab displays.
2. Inspect the **Status** field for the CTP card.

Does the **Status** field display a `Failed` message for the CTP card?

NO	YES
↓	A CTP card failure is indicated. Replace the switch. Exit MAP.

Additional analysis is not described in this MAP. Go to "MAP 0000: Start MAP" on page 30. If this is the second time at this step, contact the next level of support. Exit MAP.

MAP 0500: Port Failure and Link Incident Analysis

This MAP describes fault isolation for shortwave laser small form factor pluggable (SFP) optical transceivers, longwave laser SFP optical transceivers, and Fibre Channel link incidents. Failure indicators include:

- An event code recorded at the EWS Event Log.
- One or more amber LEDs on the ports illuminate.
- A port operational state message or a `Failed` message associated with a port at the EWS interface.

1

Was an event code **080**, **081**, **506**, **507**, **512**, **514**, **581**, **582**, **583**, **584**, **585**, or **586** observed at the EWS Event Log?

NO YES

↓ Go to step 2.

2

Table 8 lists event codes, brief explanations of the codes, and suggested actions to isolate faults.

Table 8: MAP 500 Event Codes

Event Code	Explanation	Action
080	Unauthorized worldwide name.	Go to step 12.
081	Invalid attachment.	Go to step 23.
506	Fibre Channel port failure.	Go to step 23.
507	Loopback diagnostics port failure.	Go to step 13.
512	SFP optical transceiver nonfatal error.	Go to step 13.
514	SFP optical transceiver failure.	Go to step 13.
581	Implicit incident.	Go to step 15.
582	Bit error threshold exceeded.	Go to step 15.
583	Loss of signal or loss of synchronization.	Go to step 15.

Table 8: MAP 500 Event Codes

Event Code	Explanation	Action
584	Not operational primitive sequence received.	Go to step 15.
585	Primitive sequence timeout.	Go to step 15.
586	Invalid primitive sequence received for current link state.	Go to step 15.

3

Is fault isolation being performed at the switch?

YES NO

↓ Fault isolation is being performed at the EWS interface. Go to step 6.

4

Each port has an amber LED and a blue (2 Gbps operation) or green (1 Gbps operation) LED adjacent to the port. The amber LED illuminates and the blue or green LED extinguishes if the port fails.

Is an amber port LED illuminated but not blinking (beaconing)?

YES NO

↓ The switch appears operational, however a link incident or other problem may have occurred. Go to step 15.

5

As indicated by a visual inspection, message, or event code **506**, **512**, or **514**, a Fibre Channel port failed and the SFP optical transceiver must be removed and replaced. Refer to “Remove and Replace an SFP Optical Transceiver” on page 122.

- This procedure can be performed while the switch is powered on and operational.
- Verify location of the failed port.
- Replace the optical transceiver with a transceiver of the same type (shortwave or longwave).
- Perform an external loopback test for the port as part of FRU removal and replacement. Refer to “Perform Port Diagnostic Loopback Tests” on page 98.

Did SFP optical transceiver replacement solve the problem?

NO	YES
↓	The switch appears operational. Exit MAP.

Contact the next level of support. Exit MAP.

6

Does the EWS interface appear operational?

NO	YES
↓	Go to step 9.

7

A `Page cannot be found`, `Unable to locate the server`, `HTTP 404 - file not found`, or other similar message appears. The message indicates the PC cannot communicate with the switch because:

- The switch-to-PC Ethernet link could not be established.
- AC power distribution in the switch failed, or AC power was disconnected.
- The switch CTP card failed.

Continue to the next step.

8

Ensure the switch reporting the problem is connected to facility AC power. Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated **PWR** LED (green) or **ERR** LED (amber).
- Illuminated LEDs adjacent to Fibre Channel ports.
- Audio emanations and airflow from cooling fans.

Does the switch appear powered on?

YES	NO
↓	Analysis for an Ethernet link, AC power distribution, or CTP failure is not described in this MAP. Go to "MAP 0000: Start MAP" on page 30. If this is the second time at this step, contact the next level of support. Exit MAP.

9

Inspect Fibre Channel port operational states at the EWS interface.

1. At the **View** panel, click the **Port Properties** tab. The **Port Properties** page displays with port **0** properties displayed.
2. Click the port number (**0** through **11**) for which a failure is suspected to display properties for that port.
3. Inspect the **Operational State** field. Scroll down the **View** panel as necessary.
4. Table 9 lists port operational states and MAP steps that describe fault isolation procedures.

Table 9: Port Operational States and Actions

Operational State	Action
Online	No action required. Exit MAP.
Port Failure	Go to step 9.
Offline	Go to step 10.
Not Operational	Go to step 10.
Testing	Internal or external loopback test in process. Exit MAP.
Not Installed	Go to step 11.
Invalid Attachment	Go to step 23.
Link Reset	Go to step 34.
Inactive	Go to step 35.
No light	Go to step 39.
Segmented E_Port	Go to MAP 0600: Fabric, ISL, and Segmented Port Problem Determination.

10

A switch port is unblocked and receiving the offline sequence (OLS) or not operational sequence (NOS) from an attached device.

Inform the customer that the attached device failed or is set offline. Ask the customer to take the appropriate corrective action. Exit MAP.

11

Install an SFP optical transceiver in the port receptacle. Refer to "Remove and Replace an SFP Optical Transceiver" on page 122.

- This procedure can be performed while the switch is powered on and operational.
- Verify location of the uninstalled port.
- Perform an external loopback test for the port as part of FRU removal and replacement. Refer to "Perform Port Diagnostic Loopback Tests" on page 98.

Exit MAP.

12

As indicated by a message or event code **080**, the eight-byte (16-digit) worldwide name (WWN) entered to configure port binding is not valid or a nickname was used that is not configured for the attached device. Inspect port binding parameters at the EWS interface.

1. At the **View** panel, select **Configure** at the left side of the panel. The **Configure** panel opens with the **Ports** page displayed.
2. Click the **Security** tab, then click the **Port Binding** tab. The **Port Binding** page displays.
3. Inspect entries in the **Port WWN** column. These are WWNs assigned to the port or Fibre Channel interface installed on the attached device.
   - — If a nickname is not assigned to the WWN, the WWN is prefixed by the device manufacturer's name.
   - — If a nickname is assigned to the WWN, the nickname appears in place of the WWN.
4. The bound WWN must be entered in the form of a raw WWN format (`XX:XX:XX:XX:XX:XX:XX:XX`) or must be a valid nickname. Ensure a valid WWN or nickname is entered.

Did configuring the WWN or nickname solve the problem?

NO	YES
↓	The switch appears operational. Exit MAP.

Contact the next level of support. Exit MAP.

13

As indicated by event code **507**, a Fibre Channel port failed an internal or external loopback test.

1. At the EWS interface, reset each port that failed the loopback test.
   a. At the **View** panel, select **Operations** at the left side of the panel. The **Operations** panel opens with the **Switch** and **Beacon** pages displayed.
   b. Click the **Port** tab. The **Operations** panel opens with the **Port** and **Beacon** pages displayed.
   c. Click the **Reset** tab. The **Reset** page displays.
   d. Click the check box (checked) in the **Port Reset** column and click **Activate** to reset the port. The message `Your changes have been successfully activated` appears.
2. Perform an external loopback test for all ports that were reset. Refer to "Perform Port Diagnostic Loopback Tests" on page 98.

Did resetting ports solve the problem?

NO	YES
↓	The switch appears operational. Exit MAP.

14

Port beaconing may be enabled.

1. Consult the customer and next level of support to determine the reason port beaconing is enabled.
2. Disable port beaconing at the EWS interface:
   a. At the **View** panel, select **Operations** at the left side of the panel. The **Operations** panel opens with the **Switch** and **Beacon** pages displayed.
   b. Click the **Port** tab. The **Operations** panel opens with the **Port** and **Beacon** pages displayed.
   c. Click the check box (checked) in the **Beaconing State** column and click **Activate** to remove the check mark and disable beaconing. The message `Your changes have been successfully activated` appears.

Was port beaconing enabled because port failure or degradation was suspected?

YES NO

↓ The switch appears operational. Exit MAP.

Go to step 1.

15

A link incident may have occurred. Inspect the Event Log at the EWS interface:

1. At the **View** panel, select **Monitor** at the left side of the panel. The **Monitor** panel opens with the **Port List** page displayed.
2. Click the **Log** tab. The **Log** page displays.
3. Check for event codes **581**, **582**, **583**, **584**, **585** or **586**.
4. Monitor the event log for approximately 5 minutes to determine if the link incident recurs.

Did a link incident recur?

YES NO

↓ The switch appears operational. Exit MAP.

16

A link incident has occurred and requires attention. Go to step 17.

17

Inspect the fiber-optic jumper cable attached to the port and ensure the cable is not bent and connectors are not damaged. If the cable is bent or connectors are damaged:

1. Notify the customer the port will be blocked. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the port and sets the attached device offline.
2. Block the port. Refer to "Block or Unblock a Port" on page 106.
3. Remove and replace the fiber-optic jumper cable.
4. Unblock the port. Refer to "Block or Unblock a Port" on page 106.

Was a corrective action performed?

YES NO

↓ Go to step 19.

18

Monitor port operation for approximately five minutes.

Did a link incident or **No Light** message recur?

YES NO

↓ The Fibre Channel link and switch appear operational. Exit MAP.

19

Clean fiber-optic connectors on the jumper cable.

1. Notify the customer the port will be blocked. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the port and sets the attached device offline.
2. Block the port. Refer to "Block or Unblock a Port" on page 106.
3. Disconnect both ends of the fiber-optic cable.
4. Clean the fiber-optic connectors. Refer to "Clean Fiber-Optic Components" on page 108.
5. Reconnect the fiber-optic cable.
6. Unblock the port. Refer to "Block or Unblock a Port" on page 106.
7. Monitor port operation for approximately five minutes.

Did a link incident or **No Light** message recur?

YES NO

↓ The Fibre Channel link and switch appear operational. Exit MAP.

20

Disconnect the fiber-optic jumper cable from the switch port and connect the cable to a spare port.

Does a link incident or **No Light** message display?

YES NO

↓ Go to step 22.

21

The attached device is causing the recurrent link incident or **No Light** message. Notify the customer of the problem and have the system administrator:

1. Inspect and verify operation of the attached device.
2. Repair the attached device if a failure is indicated.
3. Monitor port operation for approximately five minutes.

Did a link incident or **No Light** message recur?

YES	NO
↓	The attached device, Fibre Channel link, and switch appear operational. Exit MAP.

Contact the next level of support. Exit MAP.

22

The switch port reporting the problem is causing the recurrent link incident or **No Light** message. The recurring problem indicates port degradation and a possible pending failure. Go to step 21.

23

As indicated by a message or event code **081**, a port has an invalid attachment. The information in the **Port Properties** dialog box specifies the reason, as listed in Table 10.

Table 10: Invalid Attachment Reasons and Actions

Reason	Action
Unknown	Contact the next level of support.
ISL connection not allowed.	Go to step 24.
Incompatible switch.	Go to step 25.
External loopback plug connected.	Go to step 26.
N-Port connection not allowed.	Go to step 24.
Non-HP M-series switch at other end.	Go to step 25.
Unauthorized port binding WWN.	Go to step 12.
Unresponsive node.	Go to step 28.
Fabric binding mismatch.	Go to step 31.

Table 10: Invalid Attachment Reasons and Actions (Continued)

Reason	Action
Authorization failure reject.	Go to step 28.
Unauthorized switch binding WWN.	Go to step 32.
Fabric mode mismatch.	Go to step 25.
CNT WAN extension mode mismatch.	Go to step 33.

24

The port connection conflicts with the configured port type and an ISL connection is not allowed. Either an expansion port (E_Port) is incorrectly cabled to a Fibre Channel device or a fabric port (F_Port) is incorrectly cabled to a fabric element.

1. At the EWS interface **View** panel, select **Configure** at the left side of the panel. The **Configure** panel opens with the **Ports** page displayed.
2. At the **Type** column, click the arrow adjacent to the list box for the port and select a port type as follows:
   - — Select fabric port (**F_Port**) if the port is cabled to a device (node).
   - — Select expansion port (**E_Port**) if the port is cabled to a fabric element (director or switch) to form an ISL.
3. Click **Activate** to save the change. The message `Your changes to the Port Configuration have been successfully activated` appears.

Did reconfiguring the port type solve the problem?

NO YES

↓ The switch appears operational. Exit MAP.

Contact the next level of support. Exit MAP.

25

One of the following mode-mismatch conditions was detected and an ISL connection is not allowed:

- The switch is configured for operation in **Open Fabric 1.0** mode and is connected to a fabric element not configured to **Open Fabric 1.0** mode.
- The switch is configured for operation in **Open Fabric 1.0** mode and is connected to a legacy switch at the incorrect Exchange Link Parameter (ELP) revision level.

- The switch is configured for operation in **Open Fabric 1.0** mode and is connected to a non-HP M-series switch at the incorrect ELP revision level.
- The switch is configured for operation in **McDATA Fabric 1.0** mode and is connected to a non-HP M-series switch.

Reconfigure the switch operating mode:

1. Ensure the switch is set offline. Refer to "Set the Switch Online or Offline" on page 104.
2. At the EWS interface **View** panel, select **Configure** at the left side of the panel. The **Configure** panel opens with the **Ports** page displayed.
3. Click the **Switch** tab, then click the **Fabric Parameters** tab. The **Fabric Parameters** page displays.
4. Select **McDATA Fabric 1.0** or **Open Fabric 1.0** from the **Interop Mode** list box.
   - — Select the **McDATA Fabric 1.0** option if the switch is fabric-attached *only* to other HP directors or switches that are also operating in **McDATA Fabric 1.0** mode or **Homogeneous** mode.
   - — Select the **Open Fabric 1.0** option if the switch is fabric-attached to directors or switches produced by other original equipment manufacturers (OEMs) that are open-fabric compliant.
5. Click **Activate** to save the change. The message `Your changes to the fabric parameters configuration have been successfully activated` appears.

Did configuring the operating mode solve the problem?

NO	YES
↓	The switch appears operational. Exit MAP.

Contact the next level of support. Exit MAP.

26

A loopback (wrap) plug appears to be connected to the port and there is no diagnostic test running. Is a loopback plug in the port receptacle?

YES	NO
↓	Contact the next level of support. Exit MAP.

27

Remove the loopback plug from the port receptacle. If directed by the customer, connect a fiber-optic jumper cable attaching a device to the switch.

- If the port is operational and a device is not attached, both LEDs adjacent to the port extinguish and the port state is **No Light**.
- If the port is operational and a device is attached, the blue or green LED illuminates, the amber LED extinguishes, and the port state is **Online**.

Did removing the loopback plug solve the problem?

NO	YES
↓	The switch appears operational. Exit MAP.

Contact the next level of support. Exit MAP.

28

A port connection timed out because of an unresponsive device (node) or an ISL connection was not allowed because of a security violation (authorization failure reject). Check the port status and clean the fiber-optic connectors on the cable.

1. Notify the customer the port will be blocked. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the port and sets the attached device offline.
2. Block the port. Refer to "Block or Unblock a Port" on page 106.
3. Disconnect both ends of the fiber-optic cable.
4. Clean the fiber-optic connectors. Refer to "Clean Fiber-Optic Components" on page 108.
5. Reconnect the fiber-optic cable.
6. Unblock the port. Refer to "Block or Unblock a Port" on page 106.
7. Monitor port operation for approximately five minutes.

Is the invalid attachment problem solved?

YES	NO
↓	The Fibre Channel link and switch appear operational. Exit MAP.

29

Inspect and service the host bus adapters (HBAs) as necessary.

Did service of the HBAs solve the problem?

NO YES

↓ Exit MAP.

Contact the next level of support. Exit MAP.

30

A port connection is not allowed because of an Exchange Security Attribute (ESA) feature mismatch between two fabric elements. The SANtegrity binding feature must be enabled on both switches, and switch and fabric binding parameters must be compatible. At the EWS interface for both switches:

1. At the **View** panel, select **Configure** at the left side of the panel. The **Configure** panel opens with the **Ports** page displayed.
2. Click the **Security** tab, then click the **Switch Binding** tab. The **Switch Binding** page displays.
3. Ensure the switch binding state is enabled (noted at the top of the page) for both switches.
4. Ensure the **Connection Policy** (Enable & Restrict E_Ports, Enable & Restrict F_Ports, Enable & Restrict All Ports, or Disable Switch Binding) is compatible for both switches.
5. The **Attached Nodes** drop-down list contains the world wide names of attached Fibre Channel devices. Ensure these switch binding membership lists are compatible for both switches
   - — To add a member (node or device) to the switch binding membership list displayed at the bottom of the page, select a WWN from the **Attached Nodes** drop-down list and click the adjacent **Add Member** button; or type a new WWN in the **Detached Node (WWN)** field and click the adjacent **Add Member** button.
   - — To delete a device from the switch binding membership list, click the **Delete** button adjacent to the device WWN. A confirmation dialog box appears. Click **OK** to close the dialog box and delete the device.
6. Click **Submit**. A confirmation dialog box appears. Click **OK** to close the confirmation dialog box, activate the selected connection policy, and change the switch binding state.

7. Click the **Fabric Binding** tab. The **Fabric Binding** page displays.
8. Ensure the fabric binding membership lists are compatible for both switches
   - — To add a member (new fabric) to the fabric binding membership list displayed at the bottom of the page, type a new domain ID (range is **1** through **31**) in the **Domain ID** field, type a new WWN in the **WWN** field, and click the adjacent **Add Member** button.
   - — To delete a fabric from the fabric binding membership list, click the **Delete** button adjacent to the fabric domain ID and WWN. A confirmation dialog box appears. Click **OK** to close the dialog box and delete the fabric.
9. Click **Save and Activate** to save and activate the displayed fabric binding configuration. A confirmation dialog box appears. Click **OK** to close the confirmation dialog box, activate the fabric binding configuration, and change the status to **Saved & Active**.

Did configuring the fabric and switch binding parameters solve the problem?

NO YES

↓ The switch appears operational. Exit MAP.

Contact the next level of support. Exit MAP.

31

A port connection is not allowed because of a fabric binding mismatch between fabric elements. Fabric binding membership lists must be compatible for both switches. At the EWS interface for both switches:

1. At the **View** panel, select **Configure** at the left side of the panel. The **Configure** panel opens with the **Ports** page displayed.
2. Click the **Security** tab, then click the **Fabric Binding** tab. The **Fabric Binding** page displays.
3. Ensure the fabric binding membership lists are compatible for both switches
   - — To add a member (new fabric) to the fabric binding membership list displayed at the bottom of the page, type a new domain ID (range is **1** through **31**) in the **Domain ID** field, type a new WWN in the **WWN** field, and click the adjacent **Add Member** button.
   - — To delete a fabric from the fabric binding membership list, click the **Delete** button adjacent to the fabric domain ID and WWN. A confirmation dialog box appears. Click **OK** to close the dialog box and delete the fabric.

4. Click **Save and Activate** to save and activate the displayed fabric binding configuration. A confirmation dialog box appears. Click **OK** to close the confirmation dialog box, activate the fabric binding configuration, and change the status to **Saved & Active**.

Did updating the fabric binding membership lists solve the problem?

NO YES

↓ The switch appears operational. Exit MAP.

Contact the next level of support. Exit MAP.

32

A port connection is not allowed because of a switch binding mismatch between fabric elements. Switch membership lists must be compatible for both switches. At the EWS interface for both switches:

1. At the **View** panel, select **Configure** at the left side of the panel. The **Configure** panel opens with the **Ports** page displayed.
2. Click the **Security** tab, then click the **Switch Binding** tab. The **Switch Binding** page displays.
3. The **Attached Nodes** drop-down list contains the world wide names of attached Fibre Channel devices. Ensure these switch binding membership lists are compatible for both switches
   - — To add a member (node or device) to the switch binding membership list displayed at the bottom of the page, select a WWN from the **Attached Nodes** drop-down list and click the adjacent **Add Member** button; or type a new WWN in the **Detached Node (WWN)** field and click the adjacent **Add Member** button.
   - — To delete a device from the switch binding membership list, click the **Delete** button adjacent to the device WWN. A confirmation dialog box appears. Click **OK** to close the dialog box and delete the device.
4. Click **Submit**. A confirmation dialog box appears. Click **OK** to close the confirmation dialog box, activate the selected connection policy, and change the switch binding state.

Did updating the switch binding membership lists solve the problem?

NO YES

↓ The switch appears operational. Exit MAP.

Contact the next level of support. Exit MAP.

33

A port connection is not allowed because of a Computer Network Technologies (CNT) wide area network (WAN) extension mode mismatch. Based on switch-to-switch differences between the ELP maximum frame sizes allowed, a connection was not allowed to a switch set to CNT WAN extension mode.

CNT firmware is not currently supported by HP. Exit MAP.

34

The switch and attached device are performing a Fibre Channel link reset. This is a transient state. Wait approximately 30 seconds and inspect port state and LED behavior.

Did the link recover and resume operation?

NO YES

↓ The Fibre Channel link and switch appear operational. Exit MAP.

Go to step 1.

35

A switch port state is inactive because the Flexport Technology feature key is not installed for the port (Fibre Channel ports **4** through **11** only) or because of a transmission speed conflict between the port configuration and the SFP optical transceiver.

Is the inactive port a:

- Base configuration port (Fibre Channel ports **0** through **3**), or an
- Installed Flexport Technology port (Fibre Channel ports **4** through **11**)?

NO YES

↓ Go to step 38.

36

Does the customer desire installation of the Flexport Technology key (ports **4** through **7** and/or ports **8** through **11**)?

YES NO

↓ The switch appears operational and the **Inactive port** state is acceptable to the customer. No action is required. Exit MAP.

37

Install the Flexport Technology feature key. Refer to the *HP StorageWorks Edge Switch 2/12 Installation Guide* for more information.

Did installation of the key solve the problem?

NO YES

↓ The switch appears operational. Exit MAP.

38

A transmission speed conflict between the port configuration and the SFP optical transceiver is indicated.

1. At the EWS interface **View** panel, select **Configure** at the left side of the panel. The **Configure** panel opens with the **Ports** page displayed.
2. At the **Speed** column, click the arrow adjacent to the list box for the port and select a port speed as follows:
   - Select **1 Gb/sec** if a one gigabit per second (Gbps) optical transceiver is installed in the port.
   - Select **2 Gb/sec** if a two Gbps optical transceiver is installed in the port.
3. Click **Activate** to save the change. The message `Your changes to the Port Configuration have been successfully activated` appears.

Did reconfiguring the port speed solve the problem?

NO YES

↓ The switch appears operational. Exit MAP.

Contact the next level of support. Exit MAP.

39

A switch port state indicates **No Light** because a Fibre Channel device is not attached to the port, or a problem exists with the fiber-optic cable, attached device, or SFP optical transceiver.

Is a Fibre Channel device connected to the port?

NO YES

↓ Go to step 42.

40

Does the customer desire a device connection?

YES	NO
↓	The switch appears operational and the **No Light** state is acceptable to the customer. No action is required. Exit MAP.

41

Connect a Fibre Channel device to the port as directed by the customer.

Did connection of a device to the port solve the problem?

NO	YES
↓	The switch appears operational. Exit MAP.

42

A problem exists with the fiber-optic cable, attached device, or SFP optical transceiver. Go to step 17.

MAP 0600: Fabric, ISL, and Segmented Port Problem Determination

This MAP describes fault isolation of fabric logout, interswitch link (ISL), and E_Port segmentation problems. Failure indicators include:

- An event code recorded at the EWS Event Log.
- A segmentation reason associated with a Fibre Channel port at the EWS interface.

1

Base product Fibre Channel ports on the Edge Switch 2/12 can be configured only as F_Ports or fabric loop (Fx_Ports). Installation of the optional E_Port (or Full Fabric) feature key is required to configure ports as E_Ports and enable ISL connections to other fabric elements.

Is the E_Port (or Full Fabric) feature key installed on the switch?

NO	YES
↓	Go to step 3.

2

Does the customer want to install the E_Port (or Full Fabric) feature key?

YES NO

↓ The switch appears operational and the inability to configure E_Ports and connect the switch to another fabric element is acceptable to the customer. No action is required. Exit MAP.

Install the E_Port (or Full Fabric) feature key. Refer to the *HP StorageWorks Edge Switch 2/12 Installation Guide* for more information. Exit MAP.

3

Was an event code **011**, **021**, **051**, **052**, **061**, **062**, **063**, **070**, **071**, **072**, **140**, **142**, or **150** observed at the EWS Event Log?

YES NO

↓ Go to step 5.

4

Table 11 lists event codes, brief explanations of the codes, and suggested actions to isolate faults.

Table 11: MAP 600 Event Codes

Event Code	Explanation	Action
011	Login Server database invalid.	Go to step 7.
021	Name Server database invalid.	Go to step 7.
051	Management Server database invalid.	Go to step 8.
052	Management Server internal error.	Go to step 8.
061	Fabric Controller database invalid.	Go to step 9.
062	Maximum interswitch hop count exceeded.	Go to step 10.
063	Remote switch has too many ISLs.	Go to step 11.
070	E_Port is segmented.	Go to step 12.
071	Switch is isolated.	Go to step 12.
072	E_Port connected to unsupported switch.	Go to step 20.

Table 11: MAP 600 Event Codes (Continued)

Event Code	Explanation	Action
140	Congestion detected on an ISL.	Go to step 21.
142	Low BB_Credit detected on an ISL.	Go to step 22.
150	Zone merge failure.	Go to step 23.

5

Go to the Web browser PC accessing the switch's EWS interface.

Does the EWS interface appear operational?

YES

↓

NO

Analysis for an Ethernet link, AC power distribution, or CTP failure is not described in this MAP. Go to "MAP 0000: Start MAP" on page 30. If this is the second time at this step, contact the next level of support. Exit MAP.

6

Inspect the Fibre Channel port segmentation reason at the EWS interface.

1. At the **View** panel, click the **Port Properties** tab. The **View** panel opens with the **Port Properties** page displayed.
2. Click the port number (**0** through **11**) of the segmented port.
3. Inspect the **Reason** field for the selected port.

Is the **Reason** field blank or does it display an `N/A` message?

NO

↓

YES

The switch ISL appears operational. Exit MAP.

The **Reason** field displays a segmentation reason message. Table 12 lists the reasons and suggested actions to isolate faults.

Table 12: Port Segmentation Reasons and Actions

Segmentation Reason	Action
Incompatible operating parameters.	Go to step 13.
Duplicate domain ID.	Go to step 14.
Incompatible zoning configurations.	Go to step 15.

Table 12: Port Segmentation Reasons and Actions (Continued)

Segmentation Reason	Action
Build fabric protocol error.	Go to step 16.
No principal switch.	Go to step 18.
No response from attached switch (hello timeout).	Go to step 19.

7

A minor error occurred that caused the Fabric Services database to be re-initialized to an empty state. As a result, a disruptive fabric logout and login occurred for all attached devices. The following list explains the error:

- Event code 011 - The Login Server database failed cyclic redundancy check (CRC) validation.
- Event code 021 - The Name Server database failed CRC validation.

All attached devices resume operation after fabric login. Perform the procedure described in "Collect Maintenance Data" on page 102. Exit MAP.

8

A minor error occurred that caused the Management Server database to be re-initialized to an empty state. As a result, a disruptive server logout and login occurred for all attached devices. The following list explains the error:

- Event code 051 - The Management Server database failed CRC validation.
- Event code 052 - An internal operating error was detected by the Management Server subsystem.

All attached devices resume operation after Management Server login. Perform the procedure described in "Collect Maintenance Data" on page 102. Exit MAP.

9

As indicated by an event code **061**, a minor error occurred that caused the Fabric Controller database to fail CRC validation and be re-initialized to an empty state. As a result, the switch briefly lost interswitch link capability.

All interswitch links resume operation after CTP reset. Perform the procedure described in "Collect Maintenance Data" on page 102. Exit MAP.

10

As indicated by an event code **062**, the Fabric Controller software detected a path to another fabric element (director or switch) in a multiswitch fabric that traverses more than three interswitch links (hops). Fibre Channel frames may persist in the fabric longer than timeout values allow.

Advise the customer of the problem and work with the system administrator to reconfigure the fabric so the path between any two fabric elements does not traverse more than three hops.

Did fabric reconfiguration solve the problem?

NO YES

↓ The switch and multiswitch fabric appear operational. Exit MAP.

Contact the next level of support. Exit MAP.

11

As indicated by an event code **063**, the Fabric Controller software detected an:

- Director 2/64 in a multiswitch fabric that has more than the proscribed number of ISLs.
- Director 2/140 in a multiswitch fabric that has more than the proscribed number of ISLs.
- Other fabric element (director or switch) in a multiswitch fabric that has more than the proscribed number of ISLs.

Fibre Channel frames may be lost or routed in loops because of potential fabric routing problems. Advise the customer of the problem and work with the system administrator to reconfigure the fabric so that no director or switch elements have more than the proscribed number of ISLs.

Did fabric reconfiguration solve the problem?

NO YES

↓ The switch and multiswitch fabric appear operational. Exit MAP.

Contact the next level of support. Exit MAP.

12

A **070** event code indicates an E_Port detected an incompatibility with an attached switch and prevented the switches from forming a multiswitch fabric. A segmented E_port cannot transmit Class 2 or Class 3 Fibre Channel traffic.

A **071** event code indicates the switch is isolated from all switches in a multiswitch fabric, and is accompanied by a **070** event code for each segmented E_Port. The **071** event code is resolved when all **070** events are corrected.

Obtain supplementary event data for each **070** event code.

1. At the EWS Event Log, examine the first five bytes (**0** through **4**) of event data.
2. Byte **0** specifies the switch port number (**00** through **11**) of the segmented E_port. Byte **4** specifies the segmentation reason, as specified in Table 13.

Table 13: Byte 4 Segmentation Reasons and Actions

Byte 4	Segmentation Reason	Action
01	Incompatible operating parameters.	Go to step 13.
02	Duplicate domain ID.	Go to step 14.
03	Incompatible zoning configurations.	Go to step 15.
04	Build fabric protocol error.	Go to step 16.
05	No principal switch.	Go to step 18.
06	No response from attached switch (hello timeout).	Go to step 19.

13

A switch E_Port segmented because the error detect time out value (E_D_TOV) or resource allocation time out value (R_A_TOV) is incompatible with the attached fabric element.

1. Contact HP customer support or engineering personnel to determine the recommended E_D_TOV and R_A_TOV values for both switches.
2. Notify the customer both switches will be set offline. Ensure the system administrator quiesces Fibre Channel frame traffic through the switches and sets attached devices offline.
3. Set both switches offline. Refer to “Set the Switch Online or Offline” on page 104.
4. At the **View** panel, select **Configure** at the left side of the panel. The **Configure** panel opens with the **Ports** page displayed.
5. Click the **Switch** tab, then click the **Fabric Parameters** tab. The **Fabric Parameters** page displays.

6. Type the recommended E_D_TOV and R_A_TOV values, then click **Activate** to save the change. The message `Your changes to the fabric parameters configuration have been successfully activated` appears.
7. Repeat step 4 through step 6 for the switch attached to the segmented E_Port (second switch). Use the same E_D_TOV and R_A_TOV values.
8. Set both switches online. Refer to "Set the Switch Online or Offline" on page 104.

Did the operating parameter change solve the problem and did both switches join through the ISL to form a fabric?

NO	YES
↓	The switch, associated ISL, and multiswitch fabric appear operational. Exit MAP.

Contact the next level of support. Exit MAP.

14

A switch E_Port segmented because two fabric elements had duplicate domain IDs.

1. Work with the system administrator to determine the desired domain ID (**1** through **31** inclusive) for each switch.
2. Notify the customer both switches will be set offline. Ensure the system administrator quiesces Fibre Channel frame traffic through the switches and sets attached devices offline.
3. Set both switches offline. Refer to "Set the Switch Online or Offline" on page 104.
4. At the **View** panel, select **Configure** at the left side of the panel. The **Configure** panel opens with the **Ports** page displayed.
5. Click the **Switch** tab, then click the **Parameters** tab. The **Parameters** page displays.
6. Type the customer-determined preferred domain ID value, then click **Activate** to save the change. The message `Your changes to the Operating Parameters configuration have been successfully activated` appears.
7. Repeat step 4 through step 6 for the switch attached to the segmented E_Port (second switch). Use a different preferred domain ID value.

8. Set both switches online. Refer to "Set the Switch Online or Offline" on page 104.

Did the domain ID change solve the problem and did both switches join through the ISL to form a fabric?

NO	YES
↓	The switch, associated ISL, and multiswitch fabric appear operational. Exit MAP.

Contact the next level of support. Exit MAP.

15

A switch E_Port segmented because two switches had incompatible zoning configurations. An identical zone name is recognized in the active zone set for both switches, but the zones contain different members.

1. Work with the system administrator to determine the desired zone name change for one of the affected switches. Zone names must conform to the following rules:
   - The name must be 64 characters or fewer in length.
   - The first character must be a letter (**a** through **z**), upper or lower case.
   - Other characters must be alphanumeric (**a** through **z** or **0** through **9**), dollar sign (**$**), hyphen (**-**), caret (**^**), or underscore (_).
2. At the **View** panel, select **Configure** at the left side of the panel. The **Configure** panel opens with the **Ports** page displayed.
3. Click the **Zoning** tab, then click the **Zones** tab. The **Zones** page displays.
4. Inspect zone names (listed under **Display Previous Zones**) in the active zone set to determine the incompatible name.
5. Modify the incompatible zone name as directed by the customer. Refer to the *HP StorageWorks Edge Switch 2/12 Installation Guide* for more information on configuring zones.

Did the zone name change solve the problem and did both switches join through the ISL to form a fabric?

NO	YES
↓	The switch, associated ISL, and multiswitch fabric appear operational. Exit MAP.

Contact the next level of support. Exit MAP.

16

A switch E_Port segmented because a build fabric protocol error was detected.

1. Disconnect the fiber-optic jumper cable from the segmented E_Port.
2. Reconnect the cable to the same port.

Did disconnecting and reconnecting the cable solve the problem and did both switches join through the ISL to form a fabric?

NO	YES
↓	The switch, associated ISL, and multiswitch fabric appear operational. Exit MAP.

17

Initial machine load (IML) the switch. Refer to "IML or Reset the Switch" on page 111.

Did the IML solve the problem and did both switches join through the ISL to form a fabric?

NO	YES
↓	The switch, associated ISL, and multiswitch fabric appear operational. Exit MAP.

Perform the data collection procedure and contact the next level of support. Exit MAP.

18

A switch E_Port segmented because no switch in the fabric is capable of becoming the principal switch.

1. Notify the customer the switch will be set offline. Ensure the system administrator quiesces Fibre Channel frame traffic through the switch and sets attached devices offline.
2. Set the switch offline. Refer to "Set the Switch Online or Offline" on page 104.
3. At the **View** panel, select **Configure** at the left side of the panel. The **Configure** panel opens with the **Ports** page displayed.

4. Click the **Switch** tab, then click the **Fabric Parameters** tab. The **Fabric Parameters** page displays. The switch priority value designates the fabric's principal switch. The principal switch is assigned a priority of **1** and controls the allocation and distribution of domain IDs for all fabric switches (including itself).

   Principal is the highest priority setting, **Default** is the next highest, and **Never Principal** is the lowest priority setting. The setting **Never Principal** means that the switch is incapable of becoming a principal switch. If all switches are set to **Principal** or **Default**, the switch with the highest priority and the lowest WWN becomes the principal switch.

   At least one switch in a multiswitch fabric must be set as **Principal** or **Default**. If all switches are set to **Never Principal**, all ISLs segment and the message `No Principal Switch` appears in the **Reason** field of the **Port Properties** page.

5. At the **Switch Priority** field, select **Principal**, **Never Principal**, or **Default** (the default setting is **Default**), then click **Activate** to save the change. The message `Your changes to the Fabric Parameters configuration have been successfully activated` appears.

6. Set the switch online. Refer to "Set the Switch Online or Offline" on page 104.

Did the switch priority change solve the problem and did both switches join through the ISL to form a fabric?

NO	YES
↓	The switch, associated ISL, and multiswitch fabric appear operational. Exit MAP.

Contact the next level of support. Exit MAP.

19

A switch E_Port segmented (at an operational switch) because a response (hello timeout) to a verification check indicates an attached switch is not operational.

1. Perform the procedure described in "Collect Maintenance Data" on page 102. This information may assist in fault isolating the failed switch.

2. Go to "MAP 0000: Start MAP" on page 30 and perform fault isolation for the failed switch.

Exit MAP.

20

As indicated by an event code **072**, a switch E_Port is connected to an unsupported switch or fabric element.

Advise the customer of the problem and disconnect the interswitch link to the unsupported switch. Exit MAP.

21

A **140** event code occurs only if the optional Open Trunking feature is enabled. The event code indicates OpenTrunking firmware detected an ISL with Fibre Channel traffic that exceeds the configured congestion threshold.

No action is required for an isolated event. However, if this event persists, perform one of the following:

- Relieve the congestion by adding parallel ISLs between the switches reporting the problem.
- Increase the ISL link speed between the switches reporting the problem (from 1 Gbps to 2 Gbps).
- Reroute Fibre Channel traffic by moving device connections to a less-congested region of the fabric.

Did the corrective action solve the problem and relieve the reported ISL congestion?

NO YES

↓ The ISL appears operational. Exit MAP.

Contact the next level of support. Exit MAP.

22

A **142** event code occurs only if the optional OpenTrunking feature is enabled. The event code indicates OpenTrunking firmware detected an ISL with no transmission BB_Credit for a period of time that exceeded the configured low BB_Credit threshold. This results in downstream fabric congestion.

No action is required for an isolated event or if the reporting ISL approaches 100% throughput. However, if this event persists, perform one of the following:

- Relieve the congestion by adding parallel ISLs between the switches reporting the problem.

- Increase the ISL link speed between the switches reporting the problem (from 1 Gbps to 2 Gbps).
- Reroute Fibre Channel traffic by moving device connections to a less-congested region of the fabric.

Did the corrective action solve the problem and relieve the reported low BB_Credit condition?

NO YES

↓ The ISL appears operational. Exit MAP.

Contact the next level of support. Exit MAP.

23

A **150** event code indicates a zone merge process failed during ISL initialization. Either an incompatible zone set was detected or a problem occurred during delivery of a zone merge frame. This event code always precedes a **070** event code, and represents the reply of an adjacent fabric element in response to a zone merge frame.

Obtain supplementary event data for each **150** event code.

1. At the EWS Event Log, examine the first 12 bytes (**0** through **11**) of event data.
2. Bytes **0** through **3** specify the E_Port number (**00** through **11**) reporting the problem. Bytes **8** through **11** specify the failure reason, as specified in Table 14.

Table 14: Bytes 8 through 11 Failure Reasons and Actions

Bytes 8 - 11	Failure Reason	Action
01	Invalid data length.	Go to step 24.
08	Invalid zone set format.	Go to step 24.
09	Invalid data.	Go to step 25.
0A	Cannot merge.	Go to step 25.
F0	Retry limit reached.	Go to step 24.
F1	Invalid response length.	Go to step 24.
F2	Invalid response code.	Go to step 24.

24

A zone merge process failed during ISL initialization. The following list explains the reason:

- Failure reason 01 - An invalid data length condition caused an error in a zone merge frame.
- Failure reason 08 - An invalid zone set format caused an error in a zone merge frame.
- Failure reason F0 - A retry limit reached condition caused an error in a zone merge frame.
- Failure reason F1 - An invalid response length condition caused an error in a zone merge frame.
- Failure reason F2 - An invalid response code caused an error in a zone merge frame.

Disconnect the fiber-optic jumper cable from the E_Port reporting the problem, then reconnect the cable to the same port.

Did disconnecting and reconnecting the cable solve the problem and was the resulting zone merge process successful?

NO YES

↓ The merged zone appears operational. Exit MAP.

Perform the procedure described in "Collect Maintenance Data" on page 102. Contact the next level of support. Exit MAP.

25

A zone merge process failed during ISL initialization. The following list explains the reason:

- Failure reason 09 - Invalid data caused a zone merge failure.
- Failure reason 0A - A `Cannot Merge` condition caused a zone merge failure.

Obtain supplementary error code data for the **150** event code. At the EWS Event Log, examine bytes **12** through **15** of event data that specify the error code. Record the error code and supplementary error code data.

Perform the procedure described in "Collect Maintenance Data" on page 102. Contact the next level of support, and report the **150** event code, the associated failure reason, and the associated error code. Exit MAP.

Repair Information

3

This chapter describes the repair and repair-related procedures for the HP StorageWorks Edge Switch 2/12, and associated field replaceable units (FRUs). These procedures are performed using the EWS interface. This chapter describes:

- Procedural Notes, page 88
- Using Log Information, page 89
- Obtain Port Diagnostic Information, page 90
- Collect Maintenance Data, page 102
- Set the Switch Online or Offline, page 104
- Block or Unblock a Port, page 106
- Clean Fiber-Optic Components, page 108
- Power-On Procedure, page 109
- Power-Off Procedure, page 110
- IML or Reset the Switch, page 111
- Manage Firmware Versions, page 113
- Reset Configuration Data, page 118

Do not perform repairs until a failure is isolated to a FRU. If fault isolation was not performed, refer to “MAP 0000: Start MAP” on page 30.

Procedural Notes

The following procedural notes are referenced in applicable repair procedures. The notes do not necessarily apply to all procedures in the chapter.

1. Before performing a repair procedure, read the procedure carefully and thoroughly to familiarize yourself with the information and reduce the possibility of problems or customer down time.
2. When performing procedures described in this chapter, heed all **WARNING** and **CAUTION** statements, and other statements listed in the preface of this manual.
3. After completing steps of a detailed procedure that is referenced from another procedure, return to the initial (referencing) procedure and continue to the next step of that procedure.

Using Log Information

The EWS interface provides maintenance personnel with access to event log information for the Edge Switch 2/12.

To open the EWS event log, click the **Log** tab at the **Monitor** panel. The **Monitor** panel opens with the **Log** page displayed (Figure 16).

The log information is displayed using the following columns:

- **Date/Time** - Date and time the event occurred.
- **Error Event Code** - Three-digit code that describes the event. Event codes are listed and described in "Event Codes" on page 129.
- **Severity** - Severity of the event (**Informational**, **Minor**, **Major**, or **Severe**).
- **Event Data** - Up to 32 bytes of supplementary information (if available) in hexadecimal format. Event data is described in "Event Codes" on page 129.

You can manage log contents using the following buttons:

- **Clear Event Log Entries** - Click this button to delete all entries in the Event log.
- **Clear System Error Light** - Click the button to extinguish the System Error LED on the switch.

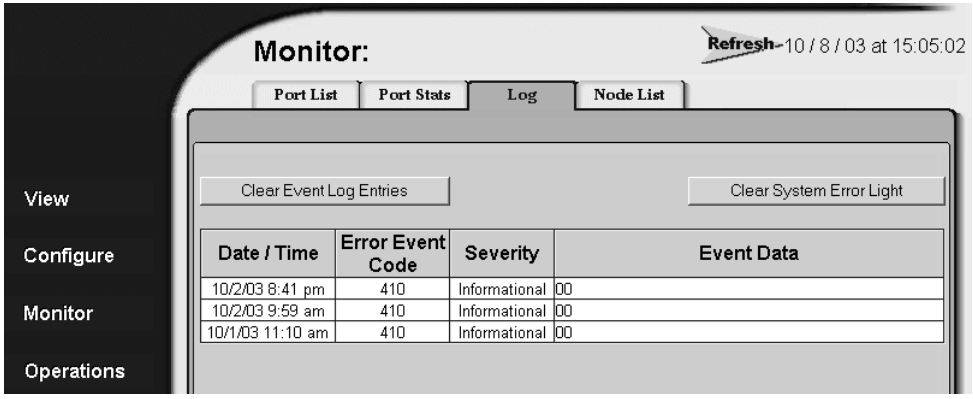

Figure 16: Monitor panel (Log page)

Obtain Port Diagnostic Information

Fibre Channel port diagnostic information can be obtained by inspecting port LEDs at the switch front panel or operating parameters at the EWS interface.

Port LEDs

To obtain port operational information, inspect port LEDs at the switch front panel. Amber and blue/green LEDs adjacent to each port indicate operational status as described in Table 15.

Table 15: Port Operational States

Port State	Blue/Green LED	Amber LED	Description
Inactive	On	Off	The port is inactive. The reason appears in the **Reason** field at the **Port Properties page** of the EWS **View panel**.
Not Installed	Off	Off	An optical transceiver is not installed in the switch port.
Not Operational	Off	Off	The port is receiving the not operational sequence (NOS) from an attached device.
Offline	Off	Off	The port is blocked and transmitting the offline sequence (OLS) to the attached device.
	Off	Off	The port is unblocked and receiving the OLS, indicating the attached device is offline.

Table 15: Port Operational States (Continued)

Port State	Blue/Green LED	Amber LED	Description
Online	On or Blinking	Off	An attached device is connected to the switch and ready to communicate, or is communicating through the switch with other attached devices. If the port remains online at 1.0625 Gbps, the blue/green LED illuminates green. If the port remains online at 2.125 Gbps, the blue/green LED illuminates blue. At the switch, the blue/green LED blinks green when there is Fibre Channel traffic through the port at 1.0625 Gbps. At the switch, the blue/green LED blinks blue when there is Fibre Channel traffic through the port at 2.125 Gbps.
Beaconing	Off, On, or Blinking	Blinking	The port is beaconing. The amber port LED blinks once every two seconds to enable users to locate the port.
Invalid Attachment	On	Off	The port has an invalid attachment. The reason appears in the **Reason** field of the **Port Properties page** of the EWS **View panel**.
Link Incident	Off	Off	A link incident occurred. The alert information appears in the EWS event log.
Link Reset	Off	Off	The switch and attached device are performing a link reset operation to recover the link connection. This is a transient state that should not persist.
No Light	Off	Off	No signal (light) is received at the switch port. This is a normal condition when there is no cable attached to the port or when the attached device is powered off.

Table 15: Port Operational States (Continued)

Port State	Blue/Green LED	Amber LED	Description
Port Failure	Off	On	The port failed and requires service.
Segmented E_Port	On	Off	The E_Port is segmented, preventing two connected switches from joining and forming a multiswitch fabric.The reason appears in the **Reason** field of the **Port Properties page** of the EWS **View panel**.
Testing	Off On	Blinking Blinking	The port is performing an internal loopback test. The port is performing an external loopback test.

EWS Interface

To obtain port operational information at the EWS interface, inspect parameters at the:

- **Monitor** Panel - **Port List** page.
- **Monitor** Panel - **Port Stats** page.
- **View** panel - **Port Properties** page.

Port List Page

When the EWS interface opens, the **View** panel appears as the default panel. At the **View** panel, select the **Monitor** option at the left side of the panel. The **Monitor** panel opens with the **Port List** page displayed (Figure 17).

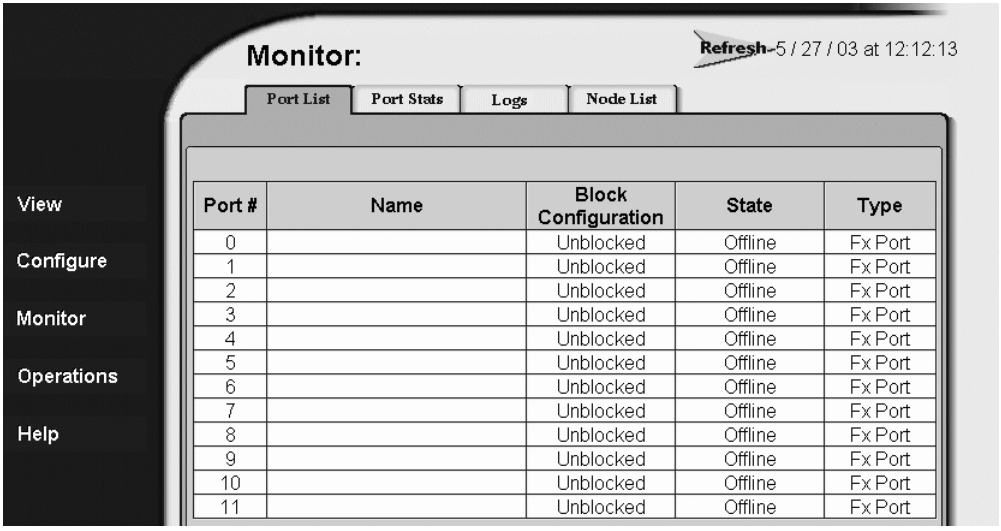

Figure 17: Monitor panel (Port List page)

A row of information for each port (**0** through **11** inclusive) appears. Each row consists of the following columns:

- **Port # -** Switch port number.
- **Name -** Port name of 24 alphanumeric characters or less. The name typically characterizes the device or fabric element to which the port is attached.
- **Block Configuration** - Indicates if a port is blocked or unblocked. Blocking a port prevents the attached devices or fabric element from communicating. A blocked port continuously transmits the offline sequence (OLS).
- **State -** Port state (**Online**, **Offline**, **Not Installed**, **Inactive**, **Invalid Attachment**, **Link Reset**, **No Light**, **Not Operational**, **Port Failure**, **Segmented E_Port**, or **Testing**).
- **Type** - Configured port type. Settings are:
  - — Fabric port (F_Port).
  - — Fabric mixed port (FX_Port). This setting also configures a port as a fabric loop port (FL_Port).
  - — Generic port (G_Port). This selection is available only if enabled through optional E_Port (or Full Fabric) feature key.

— Generic mixed port (GX_Port). This setting also configures a port as a generic loop port (GL_Port). This selection is available only if enabled through the optional E_Port (or Full Fabric) feature key.

— Expansion port (E_Port). This selection is available only if enabled through the optional E_Port (or Full Fabric) feature key.

Port Stats Page

When the EWS interface opens, the **View** panel appears as the default panel. At the **View** panel, select the **Monitor** option at the left side of the panel. The **Monitor** panel opens with the **Port List** page displayed. Click the **Port Stats** tab. The **Monitor** panel displays with the **Port Stats** page selected (Figure 18).

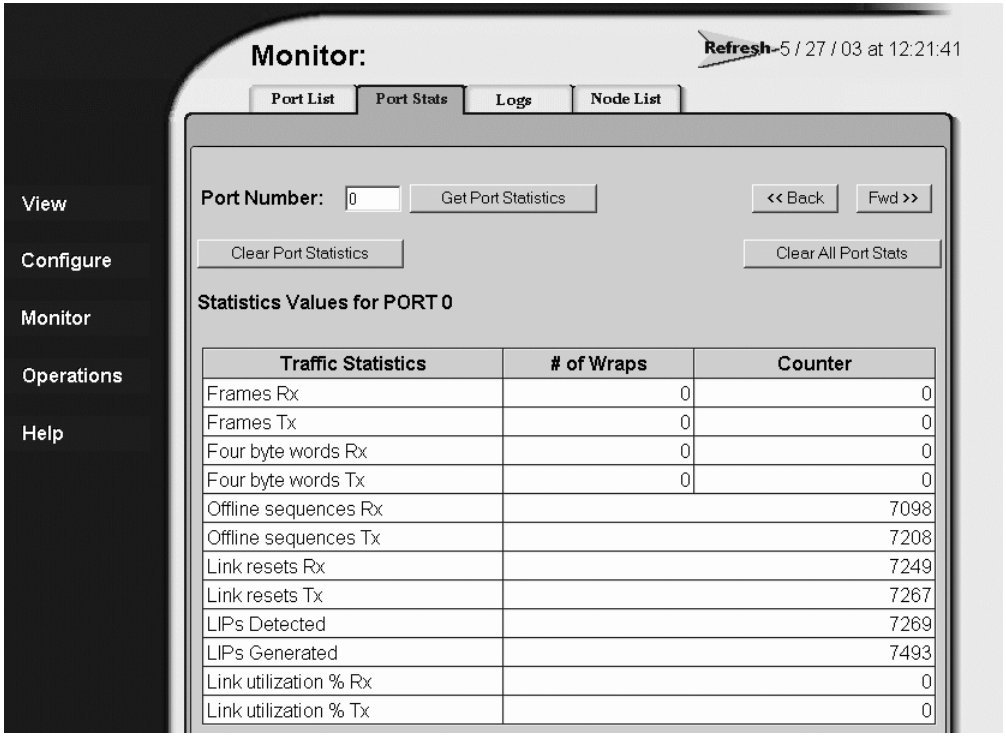

Figure 18: Monitor panel (Port Stats page)

The **Port Stats** page displays traffic and error statistics for one port. Values update only when the page opens for a selected port or the user selects **Get Port Statistics**. The page defaults to port **0**. Increment or decrement the port number displayed (**0** through **11** inclusive) by clicking **Fwd>>** or **<<Back**.

The **# of Wraps** column tracks the number of times the counter wraps for rapidly-growing statistics. The maximum counter value is 2^{32} entries. The page displays the following tables of cumulative port statistics and error count values for a selected port:

- **Traffic statistics -** These entries provide information about port traffic, including:
  - Fibre Channel frames received and transmitted.
  - Four-byte words received and transmitted.
  - Offline sequences received and transmitted.
  - Link resets received and transmitted.
  - Loop initialization primitives (LIPs) generated and detected.
  - Percent link utilization (receive and transmit).
- **Error statistics -** The **Port Stats** page displays the following error statistics for the port:
  - **Link failures -** Link failures are recorded in response to a not operational sequence (NOS), protocol timeout, or port failure.
  - **Sync losses -** Synchronization losses are detected because an attached device was reset or disconnected from the port.
  - **Signal losses -** Signal losses are detected because an attached device was reset or disconnected from the port.
  - **Primitive sequence errors -** Incorrect primitive sequences are received from an attached device, indicating Fibre Channel link-level protocol violations.
  - **Discarded frames -** Received frames could not be routed and were discarded because the frame timed out (insufficient buffer-to-buffer credit) or the destination device was not logged into the switch.
  - **Invalid transmission words -** Several transmission words were received with encoding errors, indicating an attached device is not operating in conformance with the Fibre Channel specification.

- — **CRC errors -** Received frames failed cyclic redundancy check (CRC) validation, indicating the frames arrived at the switch port corrupted. Frame corruption may be caused by device disconnection, an optical transceiver failure at the device, a bad fiber-optic cable, or a poor cable connection.
- — **Delimiter errors -** Received frames had frame delimiter errors, indicating the frame arrived at the switch port corrupted. Frame corruption may be caused by device disconnection, an optical transceiver failure at the device, a bad fiber-optic cable, or a poor cable connection.
- — **Address ID errors -** Received frames had unavailable or invalid Fibre Channel destination addresses, or invalid Fibre Channel source addresses. This typically indicates the destination device is unavailable.
- — **Frames too short -** Received frames were less than the Fibre Channel minimum size, indicating the frame arrived at the switch port corrupted. Frame corruption may be caused by device disconnection, an optical transceiver failure at the device, a bad fiber-optic cable, or a poor cable connection.

■ **Class 2 statistics -** These entries provide information about Class 2 traffic, including:

- — Class 2 frames received and transmitted.
- — Four-byte words received and transmitted.
- — Busied and rejected frames.

■ **Class 3 statistics -** These entries provide information about Class 3 traffic, including:

- — Class 3 frames received and transmitted.
- — Four-byte words received and transmitted.
- — Discarded frames.

Port Properties Page

When the EWS interface opens, the **View** panel appears as the default panel. At the **View** panel, click the **Port Properties** tab. The **View** panel displays with the **Port Properties** page selected (Figure 19).

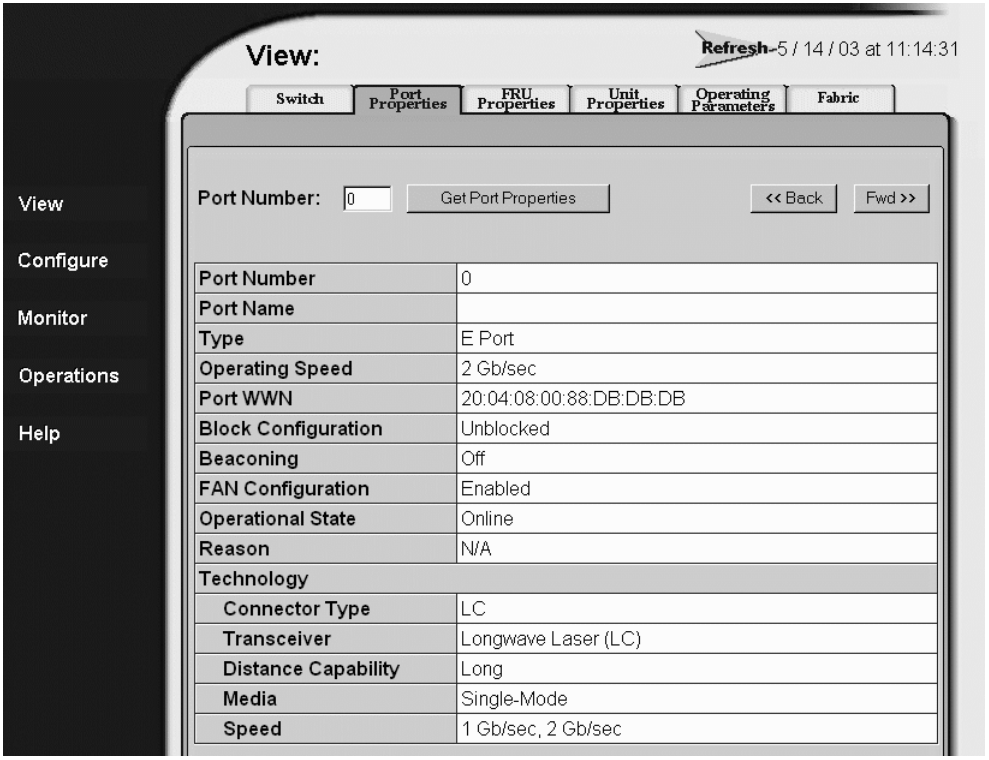

Figure 19: View panel (Port Properties page)

The **Port Properties** page displays information for one port. Values update only when the page opens for a selected port or the user selects **Get Port Properties**. The page defaults to port **0**. Increment or decrement the port number displayed (**0** through **11** inclusive) by clicking **Fwd>>** or **<<Back**. The page provides the following information:

- **Port Number -** Switch port number.
- **Port Name -** User-defined name or description for the port.
- **Type** - Port type (**GX_Port**, **FX_Port**, **G_Port**, **F_Port**, or **E_Port**).

- **Operating Speed** - Operating speed (**Not Established**, **1 Gbps**, or **2 Gbps**).
- **Port WWN -** Fibre Channel world wide name (WWN) for the port.
- **Block Configuration -** User-configured state for the port (**Blocked** or **Unblocked**).
- **Beaconing -** User-specified for the port (**On** or **Off**).
- **FAN Configuration** - User-configured state for fabric address notification (FAN) configuration (**Enabled** or **Disabled**).
- **Operational State -** Port state (**Online**, **Offline**, **Not Installed**, **Inactive**, **Invalid Attachment**, **Link Reset**, **No Light**, **Not Operational**, **Port Failure**, **Segmented E_Port**, or **Testing**).
- **Reason -** A summary appears describing the reason if the port state is **Segmented E_Port**, **Invalid Attachment**, or **Inactive**. For any other port state, the reason is **N/A**.
- **Technology -** Information specific to the installed optical transceiver, including connector type, transceiver optics, data transmission distance, optical media (cable type), and transmission speed.

Perform Port Diagnostic Loopback Tests

Port diagnostics consist of internal and external loopback tests. The tests are performed on any selected port at the EWS interface. The tests are described as follows:

- **Internal loopback test -** An internal loopback test checks internal port, serializer, and deserializer circuitry and checks for the presence of an optical transceiver, but does not check fiber-optic components of the installed transceiver. Operation of the attached device is disrupted during the test.
- **External loopback test -** An external loopback test checks all port circuitry, including fiber-optic components of the installed optical transceiver. To perform the test, the attached device must be quiesced and disconnected from the port, and a singlemode or multimode loopback plug must be inserted in the port.

Internal Loopback Test

To perform an internal loopback at the EWS interface:

1. Notify the customer that a disruptive internal loopback test is to be performed. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the port and sets the attached device offline.

Note: An SFP optical transceiver must be installed in the port during the test. A device can remain connected during the test.

---

2. When the EWS interface opens, the **View** panel and **Switch** page appear as the default. At the **View** panel, select the **Operations** option at the left side of the panel. The **Operations** panel opens with the **Switch** page displayed.
3. Click the **Port** and **Diagnostics** tabs. The **Port** page displays with the **Diagnostics** tab selected (Figure 20).

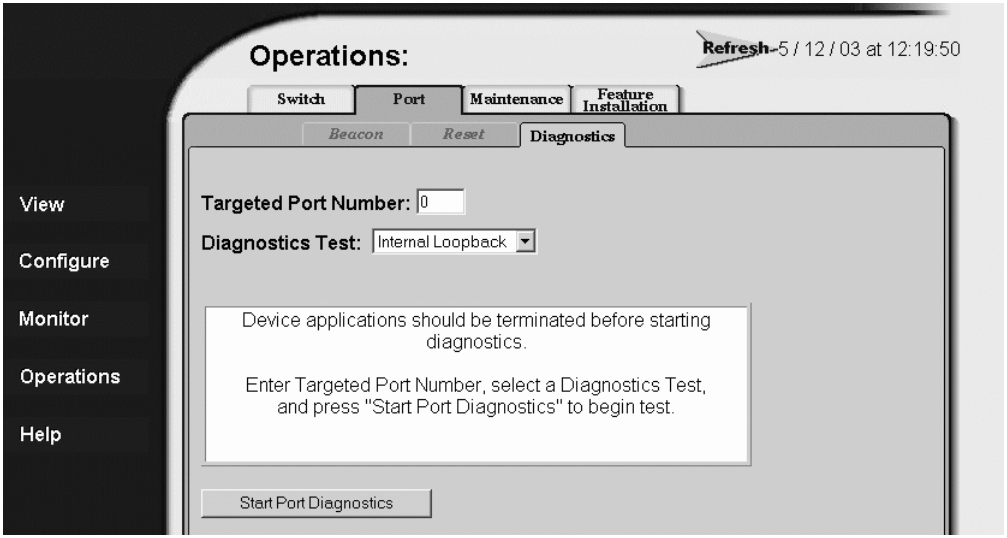

Figure 20: Operations panel (Port page with Diagnostics tab)

4. Type the port number to be tested in the **Targeted Port Number** field.
5. At the **Diagnostics Test** list box, select the **Internal Loopback** option.

6. Click **Start Port Diagnostics**. The test begins and:
   a. The **Start Port Diagnostics** button changes to a **Terminate Port Diagnostics** button.
   b. The message `Diagnostics Time Remaining: xx` appears, where `xx` are the seconds remaining in the test. The test takes approximately 30 seconds.

Note: Click **Terminate Port Diagnostics** at any time to abort the loopback test.

7. When the test completes, results appear as `Passed` or `Failed` in the message area of the dialog box.
8. Reset the tested port:
   a. Click the **Reset** tab. The **Port** page displays with the **Reset** tab selected.
   b. For the tested port, click (enable) the check box in the **Port Reset** column. A check mark in the box indicates the port reset option is enabled.
   c. Click **Activate** at the bottom of the page. The port resets and the message `Your changes have been successfully activated` appears.
9. Notify the customer the test is complete and the attached device can be set online.

External Loopback Test

To perform an external loopback at the EWS interface:

1. Notify the customer that a disruptive external loopback test is to be performed and the attached device must be disconnected.
2. Disconnect the fiber-optic jumper cable from the port to be tested.
3. Depending on the port technology, insert a singlemode or multimode loopback plug into the port receptacle.
4. When the EWS interface opens, the **View** panel and **Switch** page appear as the default. At the **View** panel, select the **Operations** option at the left side of the panel. The **Operations** panel opens with the **Switch** page displayed.
5. Click the **Port** and **Diagnostics** tabs. The **Port** page displays with the **Diagnostics** tab selected (Figure 20).

6. Type the port number to be tested in the **Targeted Port Number** field.
7. At the **Diagnostics Test** list box, select the **External Loopback** option.
8. Click **Start Port Diagnostics**. The test begins and:
   a. The **Start Port Diagnostics** button changes to a **Terminate Port Diagnostics** button.
   b. The message `Diagnostics Time Remaining: xx` appears, where `xx` are the seconds remaining in the test. The test takes approximately 30 seconds.

Note: Click **Terminate Port Diagnostics** at any time to abort the loopback test.

---

9. When the test completes, results appear as `Passed` or `Failed` in the message area of the dialog box.
10. Remove the loopback plug and reconnect the fiber-optic jumper cable from the device to the port (disconnected in step 2).
11. Reset the tested port:
    a. Click the **Reset** tab. The **Port** page displays with the **Reset** tab selected.
    b. For the tested port, click (enable) the check box in the **Port Reset** column. A check mark in the box indicates the port reset option is enabled.
    c. Click **Activate** at the bottom of the page. The port resets and the message `Your changes have been successfully activated` appears.
12. Notify the customer the test is complete and the device can be reconnected to the switch and set online.

Collect Maintenance Data

When the switch operational firmware detects a critical error, the switch automatically copies the contents of dynamic random access memory (DRAM) to a dump area in FLASH memory on the CTP card. The operator then transfers (through the Ethernet connection) the captured dump file from FLASH memory to the Web browser PC hard drive.

Perform the maintenance data collection procedure after a firmware fault is corrected or a failed FRU is replaced to capture the data for analysis by support personnel. Maintenance data includes the dump file and an engineering log viewable only by support personnel.

Note: An optional full-volatility feature is often required at military sites that process classified data. If the feature is enabled through the switch's maintenance port, a memory dump file (that possibly includes classified Fibre Channel frames) is not included as part of the data collection procedure.

To collect maintenance data (retrieve the dump file from the CTP card) at the EWS interface:

1. When the EWS interface opens, the **View** panel and **Switch** page appear as the default. At the **View** panel, select the **Operations** option at the left side of the panel. The **Operations** panel opens with the **Switch** page displayed.
2. Click the **Maintenance** and **Dump Retrieval** tabs. The **Maintenance** page displays with the **Dump Retrieval** tab selected (Figure 21).

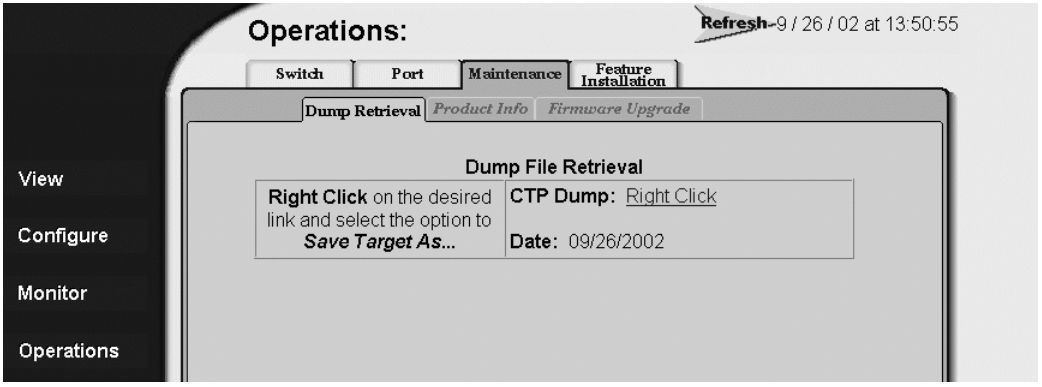

Figure 21: Operations panel (Maintenance page with Dump Retrieval tab)

3. Right-click the **CTP Dump** link to open a list of menu options.
4. Select the **Save Target As** menu option. The **Save As** dialog box displays (Figure 22).

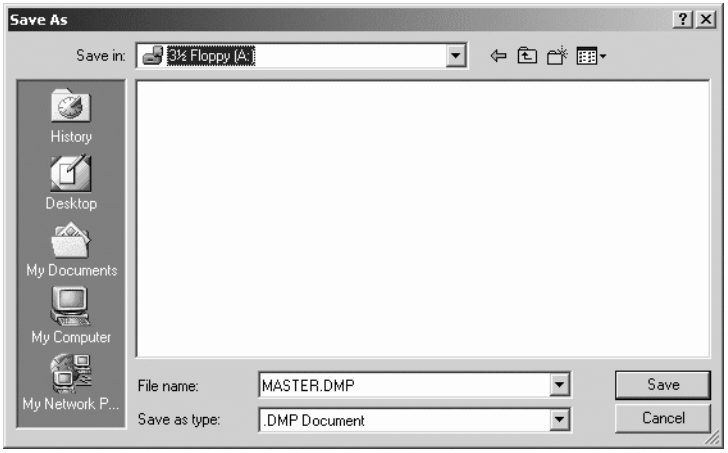

Figure 22: Save As dialog box

5. Insert a blank diskette in the floppy drive of the browser PC.
6. At the **Save As** dialog box, select the floppy drive (**A:**) from the **Save in** drop-down menu, type a descriptive name for the dump file in the **File name** field, and click **Save**.
7. A **Download** dialog box displays, showing the estimated time remaining to complete the download process. When the process finishes, the dialog box changes to a **Download complete** dialog box.
8. Click **Close** to close the dialog box.
9. Remove the diskette with the newly-collected maintenance data from the browser PC floppy drive. Return the diskette with the failed FRU to HP for failure analysis.

Set the Switch Online or Offline

This section describes procedures to set the switch online or offline. These operating states are described as follows:

- **Online -** When the switch is set online, an attached device can log in to the switch, if the port is not blocked. Attached devices can communicate with each other, if they are configured in the same zone.
- **Offline -** When the switch is set offline, all switch ports are set offline. The switch transmits the offline sequence (OLS) to attached devices, and the devices cannot log in to the switch.

Note: When the switch is set offline, the operation of attached Fibre Channel devices is disrupted. Do not set the switch offline unless directed to do so by a procedural step or the next level of support.

Set Online State

To set the switch online from the EWS interface:

1. When the EWS interface opens, the **View** panel and **Switch** page appear as the default. At the **View** panel, select the **Operations** option at the left side of the panel. The **Operations** panel opens with the **Switch** page displayed.
2. Click the **Online State** tab. The **Switch** page displays with the **Online State** tab selected (Figure 23).

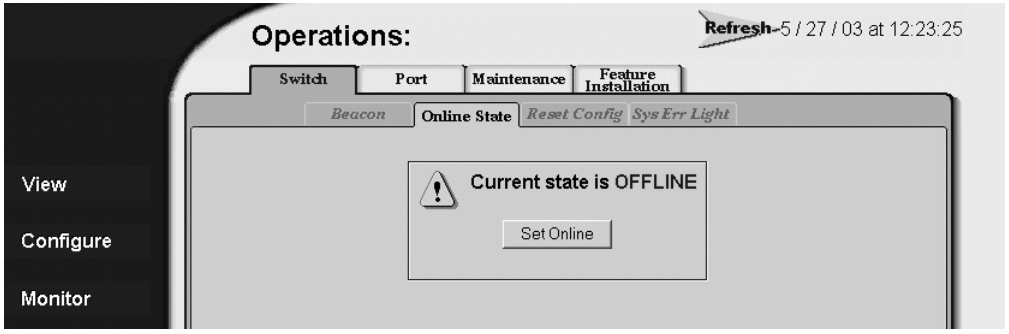

Figure 23: Operations panel (Switch page with Online State tab)

3. Click Set Online. The switch comes online and the message `Your changes have been successfully activated` appears.

Set Offline State

To set the switch offline from the EWS interface:

1. When the EWS interface opens, the **View** panel and **Switch** page appear as the default. At the **View** panel, select the **Operations** option at the left side of the panel. The **Operations** panel opens with the **Switch** page displayed.
2. Click the **Online State** tab. The **Switch** page displays with the **Online State** tab selected (Figure 23).
3. Click Set Offline. The switch goes offline and the message `Your changes have been successfully activated` appears.

Block or Unblock a Port

This section describes how to block or unblock a switch Fibre Channel port. Blocking a port prevents the attached device or fabric switch from communicating. A blocked port continuously transmits the offline sequence.

Block a Port

To block a switch port from the EWS interface:

1. When the EWS interface opens, the **View** panel and **Switch** page appear as the default. At the **View** panel, select the **Configure** option at the left side of the panel. The **Configure** panel opens with the **Ports** page displayed (Figure 24).

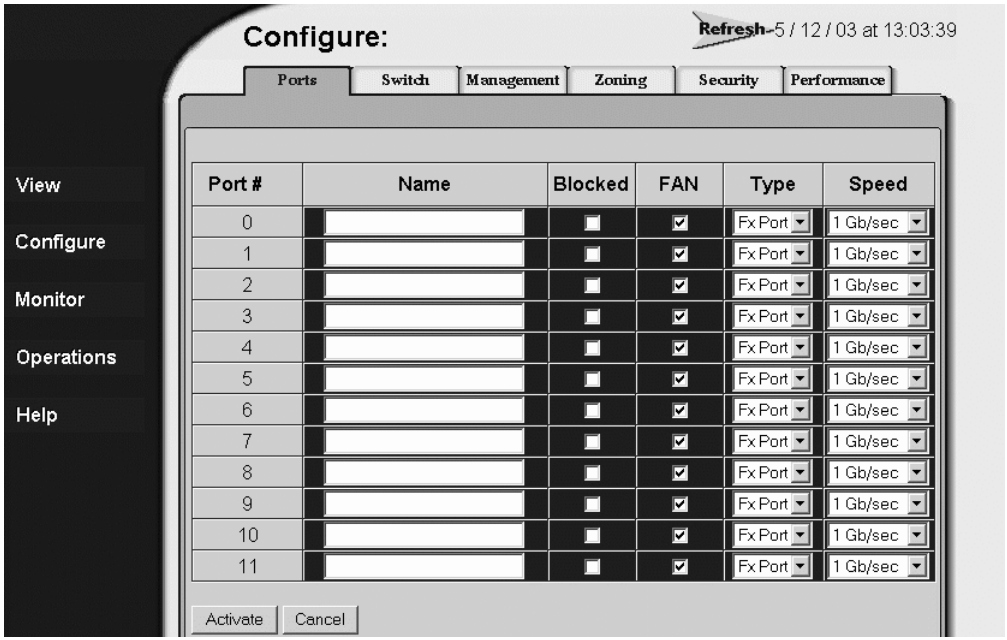

Figure 24: Configure panel (Ports page)

2. Click the check box for the selected port in the **Blocked** column to block the port (default is unblocked). A check mark indicates the port is blocked.
3. Click **Activate** at the bottom of the page to save and activate the blocked configuration. The message `Your changes to the Port Configuration have been successfully activated` appears.

Unblock a Port

To unblock a switch port from the EWS interface:

1. When the EWS interface opens, the **View** panel and **Switch** page appear as the default. At the **View** panel, select the **Configure** option at the left side of the panel. The **Configure** panel opens with the **Ports** page displayed (Figure 24).
2. Click the check box for the selected port in the **Blocked** column to remove the check mark and unblock the port. A blank box indicates the port is unblocked.
3. Click **Activate** at the bottom of the page to save and activate the unblocked configuration. The message `Your changes to the Port Configuration have been successfully activated` appears.

Clean Fiber-Optic Components

Perform this procedure as directed in this publication and when connecting or disconnecting fiber-optic cables from port optical transceivers (if necessary). To clean fiber-optic components:

1. Obtain the appropriate tools (portable can of oil-free compressed air and alcohol pads) from the fiber-optic cleaning kit.
2. Disconnect the fiber-optic cable from the transceiver. Use compressed air to blow any contaminants from the connector, as shown in part A of Figure 25.
   a. Keep the air nozzle approximately 50 millimeters (two inches) from the end of the connector and hold the can upright.
   b. Blow compressed air on the surfaces and end of the connector continuously for approximately five seconds.

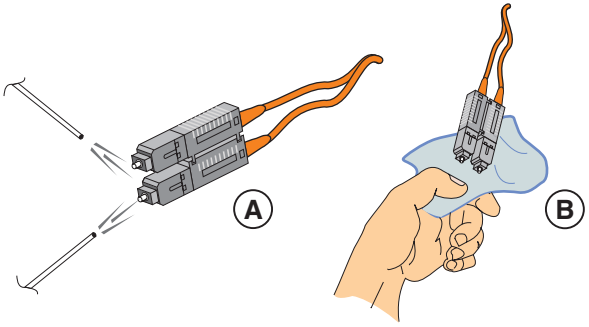

Figure 25: Clean fiber-optic components

3. Gently wipe the end-face and other surfaces of the connector with an alcohol pad as shown in part B of Figure 25. Ensure the pad makes full contact with the surface to be cleaned. Wait approximately five seconds for surfaces to dry.
4. Repeat step 2 and step 3 of this procedure (second cleaning).
5. Repeat step 2 and step 3 of this procedure again (third cleaning), then reconnect the fiber-optic cable to the port.

Power-On Procedure

To power on the switch:

1. One alternating current (AC) power cord is required for the power supply. Ensure a power cord is available to connect the switch to facility power.

WARNING: An HP power cord is provided for the Edge Switch 2/12 power supply. To prevent electric shock when connecting the switch to primary facility power, use only the supplied power cord and ensure the facility power receptacle is the correct type, supplies the required voltage, and is properly grounded.

2. Plug the power cord into a facility power source and power supply AC connector at the rear of the switch. When the power cord is connected, the switch powers on and performs power-on self-tests (POSTs).
3. During POSTs:
   - The green power (**PWR**) LED on the switch front panel illuminates.
   - The amber system error (**ERR**) LED on the switch front panel blinks momentarily while the switch is tested.
   - The green LED associated with the Ethernet port blinks momentarily while the port is tested.
   - The blue/green and amber LEDs associated with the ports blink momentarily while the ports are tested.
4. After successful POST completion, the green power (**PWR**) LED remains illuminated and all amber LEDs extinguish.
5. If a POST error or other malfunction occurs, go to "MAP 0000: Start MAP" on page 30 to isolate the problem.

Power-Off Procedure

To power off the switch:

1. Notify the customer the switch is to be powered off. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the switch and sets attached FC-AL devices offline.
2. Set the switch offline. For instructions, refer to "Set the Switch Online or Offline" on page 104.
3. Disconnect the power cord from the power supply AC connector at the rear of the switch.

IML or Reset the Switch

This section describes procedures to perform an initial machine load (IML) or reset the Edge Switch 2/12. An IML or reset is performed at the switch front panel using the recessed **IML/RESET** button.

Note: Performing an IML or switch reset does not affect the switch configuration information.

An IML does not cause power-on diagnostics to execute and is not disruptive to Fibre Channel traffic. The operation:

- Reloads switch firmware from FLASH memory.
- Resets the Ethernet LAN interface, causing the connection to the Web browser PC to drop momentarily until the connection automatically recovers.

A switch reset is more disruptive and resets the:

- Microprocessor and functional logic for the CTP card and reloads the firmware from FLASH memory.
- Ethernet LAN interface, causing the connection to the Web browser PC to drop momentarily until the connection automatically recovers.
- Ports, causing all Fibre Channel connections to drop momentarily until the connections automatically recover. This causes attached devices to log out and log back in, therefore data frames lost during switch reset must be retransmitted.

Caution: A reset should be performed only if a CTP card failure is indicated. Do not reset the switch unless directed to do so by a procedural step or the next level of support.

Switch IML

To IML the switch from the front panel:

1. Press and hold the recessed **IML/RESET** button (approximately three seconds) until the amber **ERR** LED blinks at twice the unit beaconing rate.
2. Release the button to IML the switch. During the IML, the switch-to-PC Ethernet link drops momentarily until the connection automatically recovers.

Switch Reset

To reset the switch from the front panel:

1. Press and hold the **IML/RESET** button for approximately ten seconds.
   - — After holding the button for three seconds, the amber **ERR** LED blinks at twice the unit beaoning rate.
   - — After holding the button for ten seconds, the **ERR** LED stops blinking, and all front panel LEDs illuminate.
2. Release the button to reset the switch. During the reset:
   - — The green power (**PWR**) LED on the switch front panel illuminates.
   - — The amber system error (**ERR**) LED on the switch front panel blinks momentarily while the switch is tested.
   - — The green LED associated with the Ethernet port blinks momentarily while the port is tested.
   - — The blue/green and amber LEDs associated with the ports blink momentarily while the ports are tested.
   - — The switch-to-PC Ethernet link drops momentarily until the connection automatically recovers.

Manage Firmware Versions

Firmware is the switch operating code stored in FLASH memory on the CTP card. Multiple firmware versions can be stored on a browser PC hard drive and made available for download to the switch from the EWS interface.

Service personnel can perform the following firmware management tasks from the EWS interface:

- Determine the firmware version actively running on the switch.
- Add a firmware versions to the browser PC hard drive.
- Download a firmware version to the switch.

Determine Switch Firmware Version

To determine a switch firmware version from the EWS interface:

1. When the EWS interface opens, the **View** panel and **Switch** page appear as the default. At the **View** panel, click the **Unit Properties** tab. The **Unit Properties** page displays (Figure 26).

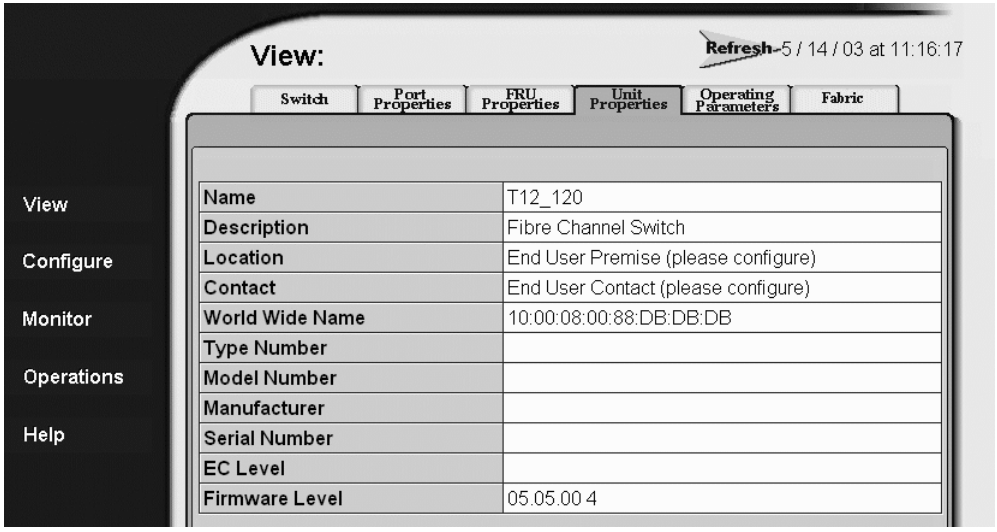

Figure 26: View panel (Unit Properties page)

2. At the bottom of the page, record the firmware version listed in the **Firmware Level** field.

Add a Firmware Version to the Browser PC Hard Drive

The firmware version shipped with the switch is provided on the Edge Switch 2/12 documentation kit CD. Subsequent firmware versions for upgrading the switch are provided to customers through the HP website.

Note: When adding a firmware version, follow all the instructions in the release notes that accompany the firmware version. This information supplements information in this general procedure.

To add a switch firmware version to the browser PC hard drive (PC running the EWS interface):

1. Obtain the new firmware version from the HP website:

Note: The following path is subject to change.

   a. At the browser PC with Internet access, open the HP website. The uniform resource locator (URL) is:

      http://hp.com/country/us/eng/support.html

   b. Follow links to the Edge Switch 2/12 firmware.

   c. Click the Edge Switch 2/12 Firmware Version XX.YY.ZZ entry, where XX.YY.ZZ is the desired version. The Windows **Save As** dialog box displays.

   d. Ensure the correct directory path is specified at the **Save** in field and the correct file is specified in the **File name** field. Click **Save**. The new firmware version is downloaded and saved to the browser PC hard drive.

2. At the browser PC, close the Internet browser session.

Download a Firmware Version to the Switch

To download a firmware version (to the switch) from the hard drive of the browser PC accessing the EWS interface:

Note: When downloading a firmware version, follow all procedural information contained in release notes or instructions that accompany the firmware version. This information supplements information provided in this general procedure.

1. When the EWS interface opens, the **View** panel and **Switch** page appear as the default. At the **View** panel, select the **Operations** option at the left side of the panel. The **Operations** panel opens with the **Switch** page displayed.
2. Click the **Maintenance** and **Firmware Upgrade** tabs. The **Maintenance** page displays with the **Firmware Upgrade** tab selected (Figure 27).

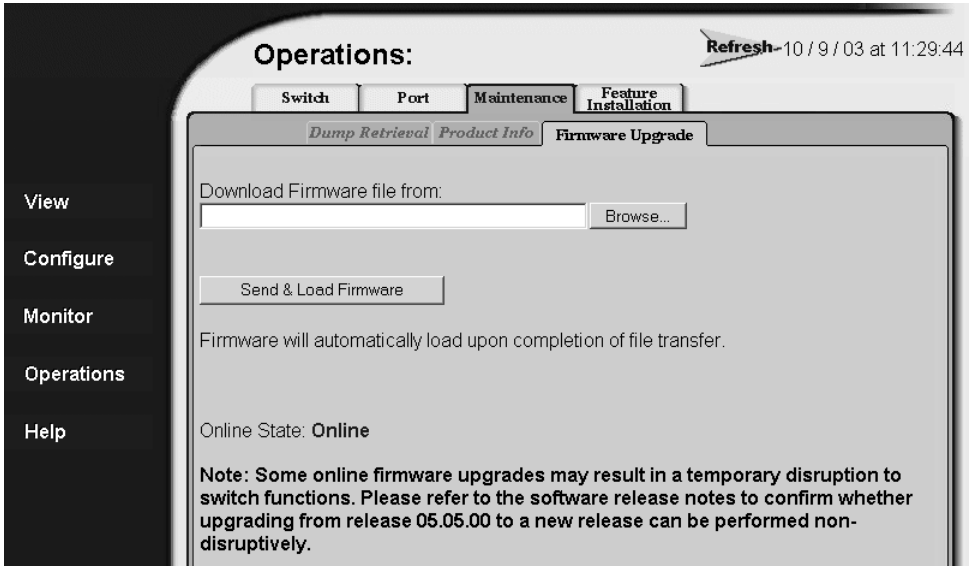

Figure 27: Operations panel (Maintenance page with Firmware Upgrade tab

3. At the **Download Firmware file from** field, do one of the following:
   - — Select the desired firmware file from the PC hard drive using the **Browse** button.
   - — Type the desired firmware filename in the **Download Firmware file from** field.
4. Click **Send and Load Firmware**. A browser-specific message box displays (Figure 28).

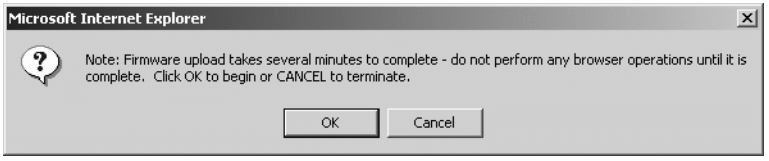
Microsoft Internet Explorer
Note: Firmware upload takes several minutes to complete - do not perform any browser operations until it is complete. Click OK to begin or CANCEL to terminate.
OK
Cancel

Figure 28: Browser-specific message box

5. Click **OK** to download the firmware version to the switch. The download process takes several minutes to complete, during which the browser is unavailable.
6. When the firmware version is downloaded to the switch and verified, the following message box displays (Figure 29).

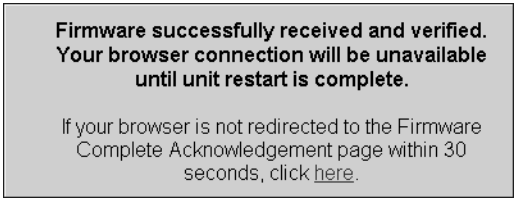
Firmware successfully received and verified.
Your browser connection will be unavailable until unit restart is complete.
If your browser is not redirected to the Firmware Complete Acknowledgement page within 30 seconds, click here.

Figure 29: Firmware Received message box

7. After firmware verification, the switch performs an IML that takes approximately 30 seconds to complete. During the IML, the browser-to-switch Ethernet connection drops momentarily and the EWS session is lost.

8. After the switch IML and EWS session logout, the following message box displays (Figure 30).

Figure 30: Firmware Upgrade Complete message box

9. Click here to login to the switch and start a new EWS session. A username and password entry dialog box displays.
10. Type the user name and password.

Note: The default user name is **Administrator** and the default password is **password.** The user name and password are case-sensitive.

---

11. Click **OK**. The EWS interface opens with the **View** panel open and the **Switch** page displayed.

Reset Configuration Data

The EWS interface provides the option to reset the configuration file to factory default values. The switch must be set offline prior to restoring the configuration file. Configuration data in the file include:

- Switch identification data.
- Port configuration data.
- Switch and fabric operating parameters.
- Simple network management protocol (SNMP) configuration information.
- Zoning configuration information.

To reset switch data to the factory default settings from the EWS interface:

Note: When switch configuration data is reset to factory default values, all optional features are disabled.

---

1. Notify the customer the switch is to be set offline. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the switch and sets attached FC-AL devices offline.
2. Set the switch offline. For instructions, refer to "Set the Switch Online or Offline" on page 104.
3. When the EWS interface opens, the **View** panel and **Switch** page appear as the default. At the **View** panel, select the **Operations** option at the left side of the panel. The **Operations** panel opens with the **Switch** page displayed.
4. Click the **Reset Config** tab. The **Switch** page displays with the **Reset Config** tab selected (Figure 31).

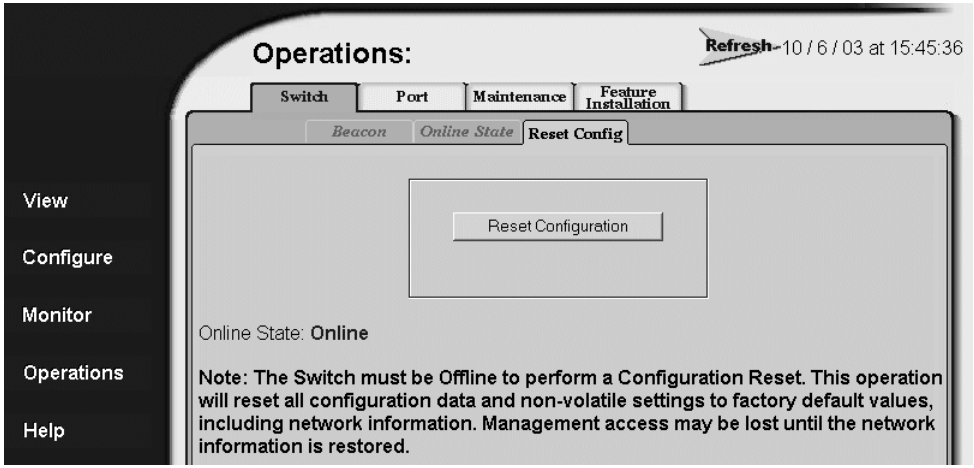

Figure 31: Operations panel (Switch page with Reset Config tab)

5. Click **Reset Configuration**. A browser-specific message box displays (Figure 32).

Microsoft Internet Explorer
Note: Resetting switch will cause loss of any user-configured settings. Click OK to reset or Cancel to terminate
OK
Cancel

Figure 32: Browser-specific message box

6. Click **OK** to reset the configuration. The message `Your changes have been successfully activated` appears.
7. The switch IP address resets to the default address of **10.1.1.10**.
   - If the configured IP address (prior to reset) was the same as the default address, the browser-to-switch Ethernet connection is not affected and the procedure is complete.
   - If the configured IP address (prior to reset) was not the same as the default address, the browser-to-switch Ethernet connection drops and the EWS session is lost. Continue to the next step.

8. To change the switch IP address and restart the EWS interface, refer to the *HP StorageWorks Edge Switch 2/12 Installation Guide*. To restart the EWS interface using the default IP address of **10.1.1.10**:
   a. At the browser, enter the default IP address of **10.1.1.10** as the Internet uniform resource locator (URL). A username and password entry dialog box displays.
   b. Type the default user name and password.

Note: The default user name is **Administrator** and the default password is **password.** The user name and password are case-sensitive.

---

   c. Click **OK**. The EWS interface opens with the **View** panel open and the **Switch** page displayed. The procedure is complete.

Optical Transceiver Removal and Replacement

4

This chapter describes removal and replacement of an SFP optical transceiver for the HP StorageWorks Edge Switch 2/12. Do not remove an SFP optical transceiver until a failure is isolated to that field replaceable unit (FRU). If fault isolation was not performed, refer to "MAP 0000: Start MAP" on page 30. This chapter describes:

- Procedural Notes, page 121
- Remove and Replace an SFP Optical Transceiver, page 122

Procedural Notes

Note the following:

1. Read the removal and replacement procedures for the FRU before removing the FRU.
2. Follow all **WARNING** and **CAUTION** statements and statements in the preface of this manual.
3. After completing a FRU replacement, clear the event code reporting the failure and the event code reporting the recovery from the switch **Event Log** at the EWS interface. Extinguish the amber system error (**ERR**) light-emitting diode (LED) at the switch front panel.

Remove and Replace an SFP Optical Transceiver

Use the following procedures to remove or replace an SFP optical transceiver from the front of the switch chassis. A list of tools required is provided.

Tools Required

The following tools are required to perform these procedures.

- Protective cap (provided with the fiber-optic jumper cable).
- Loopback plug (provided with the switch).
- Fiber-optic cleaning kit.

Removal

To remove an SFP optical transceiver:

1. Notify the customer that the port with the defective transceiver will be blocked. Ensure the customer's system administrator sets the attached device offline.
2. Identify the defective port transceiver from:
   - — The illuminated amber LED adjacent to the port.
   - — At the EWS interface, failure information associated with the port at the **Port Properties** page of the **View** panel.
3. Block communication to the port (refer to "Block or Unblock a Port" on page 106).
4. Disconnect the fiber-optic jumper cable from the port:
   a. Pull the keyed LC connector free from the port's optical transceiver.
   b. Place a protective cap over the jumper cable connector.

5. The optical transceiver has a wire locking bale to secure the transceiver in the port receptacle and to assist in removal. The locking bale rotates up or down, depending on the transceiver manufacturer and port location (top row, odd-numbered ports **1** through **11**, or bottom row, even-numbered ports **0** through **10**).
   a. Disengage the locking mechanism by rotating the wire locking bale up or down 90 degrees.
   b. Grasp the wire locking bale and pull the transceiver from the port receptacle.
6. At the Web browser connected to the EWS interface, click the **Log** tab at the **Monitor** panel. The **Event Log** displays. An event code **513** (SFP optics hot-removal completed) displays in the log.

Replacement

To replace an SFP optical transceiver:

1. Remove the replacement transceiver from its packaging.
2. Insert the transceiver into the port receptacle, then engage the locking mechanism by rotating the wire locking bale up or down 90 degrees.
3. Perform an external loopback test on the port. Refer to "Perform Port Diagnostic Loopback Tests" on page 98 for instructions. If the test fails, go to "MAP 0000: Start MAP" on page 30 to isolate the problem.
4. Reconnect the fiber-optic jumper cable:
   a. Remove the protective cap from the cable connector and the protective plug from the port's optical transceiver. Store the cap and plug in a suitable location for safekeeping.
   b. Clean the jumper cable and transceiver connectors. Refer to "Clean Fiber-Optic Components" on page 108 for instructions.
   c. Insert the keyed LC cable connector into the port's optical transceiver.
5. Ensure the amber LED adjacent to the port transceiver is extinguished. If the amber LED is illuminated, go to "MAP 0000: Start MAP" on page 30 to isolate the problem.
6. At the Web browser connected to the EWS interface, click the **Log** tab at the **Monitor** panel. The **Event Log** displays. Ensure an event code **510** (SFP optics hot-insertion initiated) displays. If the event code does not appear in the log, go to "MAP 0000: Start MAP" on page 30 to isolate the problem.

7. At the Web browser connected to the EWS interface, open the **Switch** tab at the **View** panel and:
   a. Ensure no amber LEDs illuminate that indicate a port failure.
   b. Click the graphic representing the port with the replacement transceiver to open the **Port Properties** tab. Verify port and port technology information is correct.
   c. If a problem is indicated, go to "MAP 0000: Start MAP" on page 30 to isolate the problem.
8. Restore communication to the port with the replacement transceiver as directed by the customer. Refer to "Block or Unblock a Port" on page 106 for instructions. Inform the customer the port is available.
9. To clear the system error (**ERR**) LED on the switch front bezel:
   a. Click the **Log** tab at the **Monitor** panel. The **Monitor** panel opens with the **Log** page displayed.
   b. Click the **Clear Sys Err Light** button.

Illustrated Parts Breakdown

5

This chapter provides an illustrated parts breakdown for the HP StorageWorks Edge Switch 2/12 field replaceable units (FRUs). Exploded view illustrations are provided for:

- Front-accessible FRUs
- Miscellaneous parts

Exploded-view illustrations portray the switch disassembly sequence. Illustrated FRUs are numerically keyed to associated tabular parts lists. The parts lists also include part numbers, descriptions, and quantities.

Front-Accessible FRUs

The front-accessible switch FRUs are illustrated and described in Figure 33 and Table 16. The table includes reference numbers to the figure, part numbers, descriptions, and quantities.

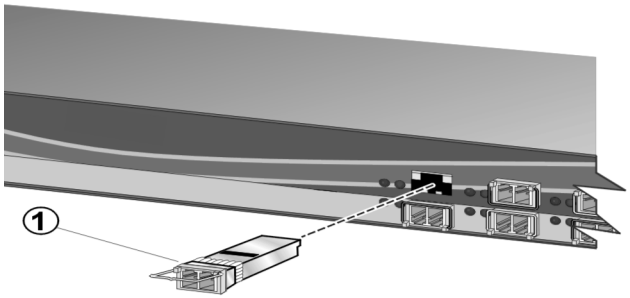

Figure 33: Front-accessible FRUs

Table 16: Front-Accessible FRU Parts List

Ref.	Part Number	Description	Qty.
N/A	348406-B21	Base assembly, Edge Switch 2/12, without optics	N/A
❶	300834-B21	Transceiver, optical, SFP, shortwave laser, LC connector, 300m, 2.125 Gbps	0 to 12
❶	300835-B21	Transceiver, optical, SFP, longwave laser, LC connector, 10 km, 2.125 Gbps	0 to 12

Miscellaneous Parts

Figure 34 illustrates miscellaneous parts. Table 17 provides the associated parts list including reference number, part number, description and quantity.

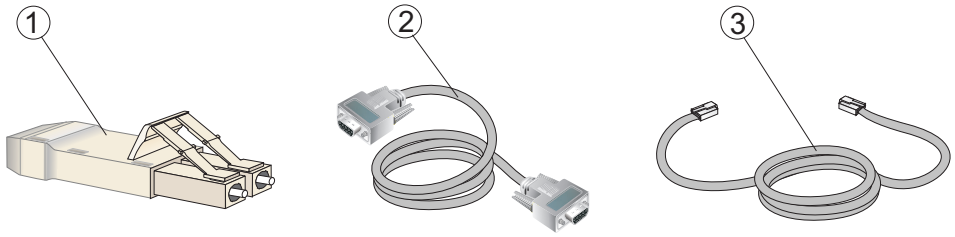

Figure 34: Miscellaneous parts

Table 17: Miscellaneous Parts

Ref.	Part Number	Description	Qty.
❶	254145-001	Plug, loopback, LC connector, multimode, 50/125 micron (#1148)	1
❶	254146-001	Plug, loopback, LC connector, singlemode, 9/125 micron (#1149)	1
❷	254144-001	Cable, null modem, DB9F-DB9F connector	1
❸	254143-001	Cable, Ethernet, 10-foot	1

Event Codes

This appendix lists all three-digit HP StorageWorks Edge Switch 2/12 event codes and provides detailed information about each code. Event codes are listed in numerical order and in tabular format.

An event is an occurrence (state change, problem detection, or problem correction) that requires user attention or that should be reported to a system administrator or service representative. An event usually indicates a switch operational state transition, but may also indicate an impending state change (threshold violation). An event may also provide information only, and not indicate an operational state change. Event codes are grouped as follows:

- **000** through **199**–system events
- **300** through **399**–fan events
- **400** through **499**–CTP card events
- **500** through **599**–port module events
- **800** through **899**–thermal

Events are recorded in the event log of the EWS interface or at a simple network management protocol (SNMP) workstation. An event may also illuminate the system error (ERR) light-emitting diode (LED) at the switch front panel.

In addition to numerical event codes, the tables in this appendix also provide the following information about each code:

- **Message–**a brief text string that describes the event.
- **Severity–**a severity level that indicates how critical an event is, as follows:
  - **0–**informational
  - **2–**minor
  - **3–**major
  - **4–**severe (not operational)
- **Explanation–**a complete explanation of what caused the event.
- **Action–**the recommended course of action (if any) to resolve the problem.
- **Event Data–**supplementary event data (if any) that displays in the event log in hexadecimal format.
- **Distribution–**check marks in associated fields indicate where the event code is reported (switch or attached host).

System Events (000 through 199)

Table 18: Event Code 011

Message:	Login Server database invalid.						
Severity:	Minor.						
Explanation:	Following an initial machine load (IML) or firmware download, the Login Server database failed its cyclic redundancy check (CRC) validation. All Fabric Services databases are initialized to an empty state, resulting in an implicit Fabric logout of all attached devices.						
Action:	Perform the procedure described in "Collect Maintenance Data" on page 102						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔					

Table 19: Event Code 021

Message:	Name Server database invalid.						
Severity:	Minor.						
Explanation:	Following an IML or firmware download, the Name Server database failed its CRC validation. All Fabric Services databases are initialized to an empty state, resulting in an implicit Fabric logout of all attached devices.						
Action:	Perform the procedure described in "Collect Maintenance Data" on page 102.						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔					

Table 20: Event Code 031

Message:	SNMP request received from unauthorized community.
Severity:	Informational.
Explanation:	An SNMP request containing an unauthorized community name was received and rejected with an error. Only requests containing authorized SNMP community names, as configured through the EWS interface, are allowed.

Table 20: Event Code 031 (Continued)

Action:	Add the community name to the SNMP configuration using the EWS interface.						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔						

Table 21: Event Code 051

Message:	Management Server database invalid.						
Severity:	Minor.						
Explanation:	Following an IML or firmware download, the Management Server database failed its CRC validation. All Management Services databases are initialized to an empty state, resulting in an implicit logout of all devices logged in to the Management Server.						
Action:	Perform the procedure described in "Collect Maintenance Data" on page 102.						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔					

Table 22: Event Code 052

<table>
<tr><td>Message:</td><td colspan="7">Management Server internal error, asynchronous status report activation, or mode register update occurred.</td></tr>
<tr><td>Severity:</td><td colspan="7">Informational.</td></tr>
<tr><td>Explanation:</td><td colspan="7">An internal operating error was detected by the Management Server subsystem, an asynchronous status was reported to an attached host, or a mode register update occurred.</td></tr>
<tr><td>Action:</td><td colspan="7">Management Server internal error: Perform the procedure described in “Collect Maintenance Data” on page 102.
Asynchronous status report activation: No action required.
Mode register update: No action required.</td></tr>
<tr><td>Event Data:</td><td colspan="7">Supplementary data consists of reporting tasks of type eMST_SB2, with component_id eMSCID_SB2_CHPGM. For each type of error or indication, the subcomponent_id is:
Management Server internal error: subcomponent_id is eMS_ELR_SB2_DEVICE_PROTOCOL_ERROR or eMS_ELR_SB2_MSG_PROCESSING_ERROR.
Asynchronous status report activation: subcomponent_id is eSB2_CP_RER_ASYNCH_STATUS_REPORTING.
Mode register update: subcomponent_id is eMS_ELR_MODE_REGISTER_UPDATE.</td></tr>
<tr><td rowspan="3">Distribution:</td><td colspan="2">Switch</td><td colspan="3">HAFM Server</td><td colspan="2">Host</td></tr>
<tr><td>EWS Event Log</td><td>System Error LED</td><td>Event Log</td><td>E-Mail</td><td>Call Home</td><td>Sense Info</td><td>Link Incident</td></tr>
<tr><td>✔</td><td></td><td></td><td></td><td></td><td>✔</td><td></td></tr>
</table>

Table 23: Event Code 061

Message:	Fabric Controller database invalid.						
Severity:	Minor.						
Explanation:	Following an IML or firmware download, the Fabric Controller database failed its CRC validation. All Fabric Controller databases are initialized to an empty state, resulting in a momentary loss of interswitch communication capability.						
Action:	Perform the procedure described in "Collect Maintenance Data" on page 102.						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔					

Table 24: Event Code 062

Message:	Maximum interswitch hop count exceeded.						
Severity:	Informational.						
Explanation:	The fabric controller software detected that a path to another fabric element (Director or Edge Switch) traverses more than seven interswitch links (ISLs or hops). This may result in Fibre Channel frames persisting in the fabric longer than standard timeout values allow.						
Action:	If possible, reconfigure the fabric so the path between any two Directors or Edge Switches traverses no more than the number of ISLs currently supported by HP. Refer to the *HP StorageWorks SAN High-Availability Planning Guide* for more information.						
Event Data:	Byte **0** = domain ID of the fabric element (Director or Edge Switch) more than seven hops away.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔						

Table 25: Event Code 063

Message:	Remote switch has too many ISLs.
Severity:	Major.
Explanation:	The fabric element (director or switch) whose domain ID is indicated in the event data has too many ISLs attached, and that element is unreachable from this switch.

Table 25: Event Code 063 (Continued)

Action:	Reduce the ISLs on the indicated fabric element to a number within the limits specified. Refer to the *HP StorageWorks SAN High-Availability Planning Guide* for more information.						
Event Data:	Byte **0** = domain ID of the fabric element (Director or Edge Switch) with too many ISLs.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔						

Table 26: Event Code 070

Message:	E_Port is segmented.
Severity:	Informational.
Explanation:	A switch E_Port recognized an incompatibility with an attached fabric element (Director or Edge Switch), preventing the switch from participating in the fabric. A segmented port does not transmit Class 2 or Class 3 traffic (data from attached devices), but transmits Class F traffic (management and control data from the attached Director or Edge Switch). Refer to event data for the segmentation reason.
Action:	Action depends on the segmentation reason specified in the event data.

Table 26: Event Code 070 (Continued)

<table>
<tr><td>Event Data:</td><td colspan="7">The first byte of event data (byte 0) specifies the E_Port number. The fifth byte (byte 4) specifies the segmentation reason as follows:
1 = Incompatible operating parameters. Either the resource allocation time out value (R_A_TOV) or error detect time out value (E_D_TOV) is inconsistent between the switch and another fabric element (Director or Edge Switch). Modify the R_A_TOV and E_D_TOV to make the values consistent for all fabric Directors and Edge Switches.
2 = Duplicate domain ID. The switch has the same preferred domain ID as another fabric element (Director or Edge Switch). Modify the switch Domain ID to make it unique.
3 = Incompatible zoning configurations. The same name is applied to a zone for the switch and another fabric element (Director or Edge Switch), but the zones contain different zone members. Modify the zone name to make it unique, or ensure zones with the same name contain identical zone members.
4 = Build fabric protocol error. A protocol error was detected during incorporation of the switch into the fabric. Disconnect the E_Port link, reconnect the link, and initial program load (IPL) the switch. If the condition persists, perform the procedure described in “Collect Maintenance Data” on page 102.
5 = No principal switch. No Director or Edge Switch in the fabric can become the principal switch. Modify the switch priority to any value other than 255.
6 = No response from attached switch (hello timeout). The switch periodically verifies operation of attached fabric elements (Director or Edge Switch). The switch E_Port (at the operational switch) times out and segments if the attached device does not respond. Check the status of the attached Director or Edge Switch. If the condition persists, perform the procedure described in “Collect Maintenance Data” (at the attached device) on page 102.</td></tr>
<tr><td rowspan="3">Distribution:</td><td colspan="2">Switch</td><td colspan="3">HAFM Server</td><td colspan="2">Host</td></tr>
<tr><td>EWS Event Log</td><td>System Error LED</td><td>Event Log</td><td>E-Mail</td><td>Call Home</td><td>Sense Info</td><td>Link Incident</td></tr>
<tr><td>✔</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

Table 27: Event Code 071

<table>
<tr><td>Message:</td><td colspan="7">Switch is isolated.</td></tr>
<tr><td>Severity:</td><td colspan="7">Informational.</td></tr>
<tr><td>Explanation:</td><td colspan="7">The switch is isolated from other fabric elements (Director or Edge Switch). This event code is accompanied by one or more 070 event codes. Refer to the event data for the segmentation reason.</td></tr>
<tr><td>Action:</td><td colspan="7">Action depends on the segmentation reason specified in the event data.</td></tr>
<tr><td>Event Data:</td><td colspan="7">The first byte of event data (byte 0) specifies the E_Port number. The fifth byte (byte 4) specifies the segmentation reason as follows:
1 = Incompatible operating parameters. Ether the resource allocation time out value (R_A_TOV) or error detect time out value (E_D_TOV) is inconsistent between the switch and another fabric element (Director or Edge Switch). Modify the R_A_TOV and E_D_TOV to make the values consistent for all fabric Directors and Edge Switches.
2 = Duplicate domain ID. The switch has the same preferred domain ID as another fabric element (Director or Edge Switch). Modify the switch's Domain ID to make it unique.
3 = Incompatible zoning configurations. The same name is applied to a zone for the switch and another fabric element (Director or Edge Switch), but the zones contain different zone members. Modify the zone name to make it unique, or ensure zones with the same name contain identical zone members.</td></tr>
<tr><td>Event Data (continued):</td><td colspan="7">4 = Build fabric protocol error. A protocol error was detected during incorporation of the switch into the fabric. Disconnect the E_Port link, reconnect the link, and IML the switch. If the condition persists, perform the procedure described in "Collect Maintenance Data" on page 102.
5 = No principal switch. No Director or Edge Switch in the fabric can become the principal switch. Modify the switch priority to any value other than 255.
6 = No response from attached switch (hello timeout). The switch periodically verifies operation of attached fabric elements (Director or Edge Switch). The switch E_Port (at the operational switch) times out and segments if the attached device does not respond. Check the status of the attached Director or Edge Switch. If the condition persists, perform the procedure described in "Collect Maintenance Data" (at the attached device) on page 102.</td></tr>
<tr><td rowspan="2">Distribution:</td><td colspan="2">Switch</td><td colspan="3">HAFM Server</td><td colspan="2">Host</td></tr>
<tr><td>EWS Event Log</td><td>System Error LED</td><td>Event Log</td><td>E-Mail</td><td>Call Home</td><td>Sense Info</td><td>Link Incident</td></tr>
<tr><td></td><td>✔</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

Table 28: Event Code 072

Message:	E_Port connected to unsupported switch.						
Severity:	Informational.						
Explanation:	The switch is attached (through an ISL) to an incompatible fabric element (Director or Edge Switch).						
Action:	Disconnect the ISL.						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔						

Table 29: Event Code 073

Message:	Fabric initialization error.						
Severity:	Informational.						
Explanation:	An error was detected during the fabric initialization sequence, most likely caused by frame delivery errors. Event data is intended for engineering evaluation.						
Action:	Perform the procedure described in "Collect Maintenance Data" on page 102.						
Event Data:	Byte **0** = error reason code for engineering evaluation. Bytes **4**–**9** = port numbers for which problems were detected.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔						

Table 30: Event Code 074

Message:	ISL frame delivery error threshold exceeded.						
Severity:	Informational.						
Explanation:	Fabric controller frame delivery errors exceeded an E_Port threshold and caused fabric initialization problems (**073** event code). Most fabric initialization problems are caused by control frame delivery errors, as indicated by this code. Event data is intended for engineering evaluation.						
Action:	Perform the procedure described in "Collect Maintenance Data" on page 102.						
Event Data:	Byte **0** = E_Port number reporting the problem. Bytes **4–8** = Count of frame delivery timeouts. Bytes **9–11** = Count of frame delivery aborts.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔						

Table 31: Event Code 080

Message:	Unauthorized world-wide name.						
Severity:	Informational.						
Explanation:	The world-wide name of the device or switch plugged in the indicated port is not authorized for that port.						
Action:	Change the port binding definition or plug the correct device or switch into this port.						
Event Data:	Byte **0** = Port number reporting the unauthorized connection. Bytes **1–3** = reserved. Bytes **4–11** = WWN of the unauthorized device or fabric element.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔					✔	

Table 32: Event Code 081

Message:	Invalid attachment.
Severity:	Informational.
Explanation:	A switch port recognized an incompatibility with the attached fabric element or device and isolated the port. An isolated port does not transmit Class 2, Class 3, or Class F traffic. Refer to the event data for the reason.
Action:	Action depends on the reason specified in the event data.
Event Data:	The first byte of event data (byte **0**) specifies the port number. The fifth byte (byte **4**) specifies the isolation reason as follows: **1 = Unknown**–Isolation reason is unknown, but probably caused by failure of a device attached to the switch through an E_Port connection. Fault isolate the failed device or contact support personnel to report the problem. **2 = ISL connection not allowed**–The port connection conflicts with the configured port type. Change the port type to F_Port if the port is cabled to a device, or E_Port if the port is cabled to a fabric element to form an ISL. **3 = Incompatible switch**–The switch returned a `Process ELP Reject-Unable to Process` reason code because the attached fabric element is not compatible. If the established switches are already operating in McDATA Fabric 1.0 (also known as Homogeneous mode when managing the SAN using HAFM), set the switch operating mode to that mode. Otherwise, set the switch operating mode to Open Fabric 1.0 if connected to M-Series Fabric Directors or Edge Switches in Open Fabric 1.0 mode, or an Open Fabric-compliant product manufactured by a different vendor. **4 = Incompatible switch**–The switch returned a `Process ELP Reject-Invalid Revision Level` reason code because the attached fabric element is not compatible. If the established switches are already operating in McDATA Fabric 1.0 (also known as Homogeneous mode when managing the SAN using HAFM), set the switch operating mode to that mode. Otherwise, set the switch operating mode to Open Fabric 1.0 if connected to M-Series Fabric directors or edge switches in Open Fabric 1.0 mode, or an Open Fabric-compliant product manufactured by a different vendor. **5 = Loopback plug connected**–A loopback plug is connected to the port with no diagnostic test running. Remove the loopback plug. **6 = N_Port connection not allowed**–The switch is connected to a fabric element through a port configured as an F_Port. Change the port type to E_Port. **7 = Non-HP M-series switch at other end**–The attached fabric element is not an HP M-series switch. Set the switch operating mode to Open Fabric 1.0 if connected to an Open Fabric-compliant product manufactured by a different vendor. **A = Unauthorized port binding WWN**–The device WWN or nickname used to configure port binding for this port is not valid. Reconfigure the port with the WWN or nickname authorized for the attached device.

Table 32: Event Code 081 (Continued)

<table>
<tr><td></td><td colspan="7">**B = Unresponsive node**–The attached node did not respond, resulting in a G_Port ELP timeout. Check the status of the attached device and clean the link's fiber-optic components (cable and connectors). If the problem persists, contact support personnel to report the problem.

C = ESA security mismatch–Processing of the Exchange Security Attribute (ESA) frame detected a security feature mismatch. The fabric binding and switch binding parameters for this switch and the attached fabric element must agree. At the **Fabric Binding** and **Switch Binding–State Change** dialog boxes, ensure the parameters for both fabric elements are compatible, or disable the fabric and switch binding features.

D = Fabric binding mismatch–Fabric binding is enabled and an attached fabric element has an incompatible fabric membership list. At the **Fabric Binding** dialog box, update the fabric membership list for both fabric elements to ensure compatibility, or disable the fabric binding feature.

E = Authorization failure reject–The fabric element connected to the switch through an ISL detected a security violation. As a result, the switch received a generic reason code and set the port to an invalid attachment state. Check the port status of the attached fabric element and clean the link's fiber-optic components (cable and connectors). If the problem persists, contact support personnel to report the problem.

F = Unauthorized switch binding WWN–Switch binding is enabled and an attached device or fabric element has an incompatible switch membership list. At the **Switch Binding–Membership List** dialog box, update the switch membership list for the switch and the attached device or fabric element to ensure compatibility, or disable the switch binding feature.

11 = Fabric mode mismatch–Based on the ELP revision level, a connection was not allowed because an HP switch in legacy mode is attached to an HP switch in Open Fabric mode, or an HP switch in Open Fabric mode is attached to an OEM switch at an incorrect ELP revision level. Update the fabric mode for one switch using the **Interop Mode** drop-down list at the **Configure Fabric Parameters** dialog box.

12 = CNT WAN extension mode mismatch–Based on switch-to-switch differences between the ELP maximum frame sizes allowed, a connection was not allowed to a switch set to Computer Network Technologies (CNT) wide area network (WAN) extension mode. CNT firmware is not currently supported by HP.</td></tr>
<tr><td rowspan="2">Distribution:</td><td colspan="2">Switch</td><td colspan="3">HAFM Server</td><td colspan="2">Host</td></tr>
<tr><td>EWS Event Log</td><td>System Error LED</td><td>Event Log</td><td>E-Mail</td><td>Call Home</td><td>Sense Info</td><td>Link Incident</td></tr>
<tr><td></td><td>✔</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

Table 33: Event Code 120

Message:	Error detected while processing system management command.						
Severity:	Informational.						
Explanation:	This event occurs when the switch receives a management command that violates specified boundary conditions, typically as a result of a network error. The switch rejects the command, drops the switch-to-server Ethernet link, and forces error recovery processing. When the link recovers, the command can be retried.						
Action:	No action is required for an isolated event. If this event persists, perform the procedure described in "Collect Maintenance Data" on page 102.						
Event Data:	No supplementary data included with the event.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔						

Table 34: Event Code 121

Message:	Zone set activation failed–zone set too large.						
Severity:	Informational.						
Explanation:	This event occurs when the switch receives a zone set activation command that exceeds the size supported by the switch. The switch rejects the command, drops the switch-to-server Ethernet link, and forces error recovery processing. When the link recovers, the command can be modified and retried.						
Action:	Reduce the size of the zone set to conform to the limit specified, then retry the activation command.						
Event Data:	No supplementary data included with the event.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔						

Table 35: Event Code 140

Message:	Congestion detected on an ISL.						
Severity:	Informational.						
Explanation:	Open Trunking firmware detected an ISL with Fibre Channel traffic that exceeded the configured congestion threshold.						
Action:	No action is required for an isolated event. If this event persists, relieve the congestion by adding parallel ISLs, increasing the ISL link speed, or moving device connections to a less-congested region of the fabric.						
Event Data:	Byte 0 = Port number reporting congestion.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔						

Table 36: Event Code 141

Message:	Congestion relieved on an ISL.						
Severity:	Informational.						
Explanation:	Open Trunking firmware detected an ISL with Fibre Channel traffic that previously exceeded the configured congestion threshold. The congestion is now relieved.						
Action:	No action required.						
Event Data:	Byte 0 = Port number reporting congestion relieved.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔						

Table 37: Event Code 142

Message:	Low BB_Credit detected on an ISL.						
Severity:	Informational.						
Explanation:	Open Trunking firmware detected an ISL with no transmission BB_Credit for a period of time that exceeded the configured low BB_Credit threshold. This indicates downstream fabric congestion.						
Action:	No action is required for an isolated event or if the reporting ISL approaches 100% throughput. If this event persists, relieve the low BB_Credit condition by adding parallel ISLs, increasing the ISL link speed, or moving device connections to a less-congested region of the fabric.						
Event Data:	Byte 0 = Port number reporting low BB_Credit.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔						

Table 38: Event Code 143

Message:	Low BB_Credit relieved on an ISL.						
Severity:	Informational.						
Explanation:	Open Trunking firmware detected an ISL with no transmission BB_Credit for a period of time that previously exceeded the configured low BB_Credit threshold. The low-credit condition is now relieved.						
Action:	No action required.						
Event Data:	Byte 0 = Port number reporting low BB_Credit relieved.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔						

Table 39: Event Code 150

Message:	Zone merge failure.
Severity:	Informational.
Explanation:	During ISL initialization, the zone merge process failed. Either an incompatible zone set was detected or a problem occurred during delivery of a zone merge frame. This event code always precedes a 070 ISL segmentation event code, and represents the reply of an adjacent fabric element in response to a zone merge frame. Refer to the event data for the failure reason.
Action:	Action depends on the failure reason specified in the event data.
Event Data:	Bytes 0–3 of the event data specify affected E_Port number(s). Bytes 8–11 specify the failure reason as follows: 01 = Invalid data length–An invalid data length condition caused an error in a zone merge frame. Disconnect the E_Port link, then reconnect the link. If the condition persists, perform the procedure described in "Collect Maintenance Data" on page 102. 08 = Invalid zone set format–An invalid zone set format caused an error in a zone merge frame. Disconnect the E_Port link, then reconnect the link. If the condition persists, perform the procedure described in "Collect Maintenance Data" on page 102. 09 = Invalid data–Invalid data caused a zone merge failure. Inspect bytes 12–15 of the event data for error codes. Refer to error code definitions listed on the following page to correct the problem. 0A = Cannot merge–A `Cannot Merge` condition caused a zone merge failure. Inspect bytes 12–15 of the event data for error codes. Refer to error code definitions listed on the following page to correct the problem. F0 = Retry limit reached–A retry limit reached condition caused an error in a zone merge frame. Disconnect the E_Port link, then reconnect the link. If the condition persists, perform the procedure described in "Collect Maintenance Data" on page 102. F1 = Invalid response length–An invalid response length condition caused an error in a zone merge frame. Disconnect the E_Port link, then reconnect the link. If the condition persists, perform the procedure described in "Collect Maintenance Data" on page 102. F2 = Invalid response code–An invalid response code caused an error in a zone merge frame. Disconnect the E_Port link, then reconnect the link. If the condition persists, perform the procedure described in "Collect Maintenance Data" on page 102.

Table 39: Event Code 150

<table>
<tr><td colspan="8">Event Code: 150 (continued)</td></tr>
<tr><td>Event Data (continued):</td><td colspan="7">Bytes 12–15 of the event data specify error codes as follows:
01 = Completion fail.
03 = Zone merge error–too many zones.
04 = Zone merge error–incompatible zones.
05 = Zone merge error–too long if reason = 0A.
06 = Zone set definition too long.
07 = Zone set name too short or not authorized.
08 = Invalid number of zones.
09 = Zone merge error–default zone states incompatible if reason = 0A.
0A = Invalid protocol.
0B = Invalid number of zone members.
0C = Invalid flags.
0D = Invalid zone member information length.
0E = Invalid zone member information format.
0F = Invalid zone member information port.
10 = Invalid zone set name length.
11 = Invalid zone name length.
37 = Invalid zone name.
39 = Duplicate zone.
3C = Invalid number of zone members.
3D = Invalid zone member type.
3E = Invalid zone set name.
45 = Duplicate member in zone.
4A = Invalid number of zones.
4B = Invalid zone set size.
4D = Maximum number of unique zone members exceeded.</td></tr>
<tr><td rowspan="3">Distribution:</td><td colspan="2">Switch</td><td colspan="3">HAFM Server</td><td colspan="2">Host</td></tr>
<tr><td>EWS Event Log</td><td>System Error LED</td><td>Event Log</td><td>E-Mail</td><td>Call-Home</td><td>Sense Info</td><td>Link Incident</td></tr>
<tr><td>✔</td><td>✔</td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

Table 40: Event Code 151

<table>
<tr><td>Message:</td><td colspan="7">Fabric configuration failure.</td></tr>
<tr><td>Severity:</td><td colspan="7">Informational.</td></tr>
<tr><td>Explanation:</td><td colspan="7">A fabric-wide configuration activation process failed. An event code 151 is recorded only by the managing switch in the fabric. The event code is intended to help engineering support personnel fault isolate fabric-wide configuration failures.</td></tr>
<tr><td>Action:</td><td colspan="7">Perform the procedure described in “Collect Maintenance Data” on page 102.</td></tr>
<tr><td>Event Data:</td><td colspan="7">Event data are mapped from the software implementation of the FC-SW2 protocol and are typically complicated. Decoding the event data requires engineering support. Event data are as follows:

Bytes 0 - 3 = Managing switch domain ID in internal format (1-31).
Bytes 4 - 7 = Fabric configuration operation that failed.
Bytes 8 - 11 = Fabric configuration step that failed.
Bytes 12 - 15 = Managed switch domain ID in internal format (1-31).
Bytes 16 - 19 = Response command code received from the managed switch.
Bytes 20 - 23 = Response code received from the managed switch.
Bytes 24 - 27 = Reason code received from the managed switch.
Bytes 28 - 31 = Error code received from the managed switch.</td></tr>
<tr><td rowspan="2">Distribution:</td><td colspan="2">Switch</td><td colspan="3">HAFM Server</td><td colspan="2">Host</td></tr>
<tr><td>EWS Event Log</td><td>System Error LED</td><td>Event Log</td><td>E-Mail</td><td>Call Home</td><td>Sense Info</td><td>Link Incident</td></tr>
<tr><td></td><td>✔</td><td>✔</td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

Fan Module Events (300 through 399)

Table 41: Event Code 300

Message:	Cooling fan propeller failed.						
Severity:	Major.						
Explanation:	One cooling fan (out of three) failed or is rotating at insufficient angular velocity. The remaining fans are operational. The amber LED illuminates at the rear of the power supply assembly associated with the failed fan.						
Action:	Replace the switch.						
Event Data:	The first byte of event data (byte **0**) specifies the failed fan number (**0** through **2** inclusive).						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔				✔	

Table 42: Event Code 301

Message:	Cooling fan propeller failed.						
Severity:	Major.						
Explanation:	Two cooling fans (out of three) failed or are rotating at insufficient angular velocity. The remaining fans are operational. The amber LED illuminates at the rear of the power supply assembly (or assemblies) associated with the failed fans.						
Action:	Replace the switch.						
Event Data:	The first byte of event data (byte **0**) specifies the failed fan numbers (**0** through **2** inclusive).						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔				✔	

Table 43: Event Code 302

Message:	Cooling fan propeller failed.						
Severity:	Major.						
Explanation:	Three cooling fans (out of three) failed or are rotating at insufficient angular velocity. The remaining fans are operational. The amber LED illuminates at the rear of the power supply assembly (or assemblies) associated with the failed fans.						
Action:	Replace the switch.						
Event Data:	The first byte of event data (byte **0**) specifies the failed fan numbers (**0** through **2** inclusive).						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔				✔	

Table 44: Event Code 310

Message:	Cooling fan propeller recovered.						
Severity:	Informational.						
Explanation:	One cooling fan (out of three) recovered. All fans are operational.						
Action:	No action required.						
Event Data:	The first byte of event data (byte **0**) specifies the recovered fan number (**0** through **2** inclusive).						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔						

Table 45: Event Code 311

Message:	Cooling fan propeller recovered.						
Severity:	Informational.						
Explanation:	Two cooling fans (out of three) recovered. All fans are operational.						
Action:	No action required.						
Event Data:	The first byte of event data (byte **0**) specifies the recovered fan numbers (**0** through **2** inclusive).						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error Indicator	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔						

Table 46: Event Code 312

Message:	Cooling fan propeller recovered.						
Severity:	Informational.						
Explanation:	Three cooling fans (out of three) recovered. All fans are operational.						
Action:	No action required.						
Event Data:	The first byte of event data (byte **0**) specifies the recovered fan numbers (**0** through **2** inclusive).						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔						

CTP Card Events (400 through 499)

Table 47: Event Code 400

Message:	Power-up diagnostics failure.						
Severity:	Major.						
Explanation:	Power-on self tests (POSTs) detected a faulty field replaceable unit (FRU) as indicated by the event data.						
Action:	If a CTP card failure is indicated, replace the switch. If a fan or power supply failure is indicated, replace the switch. Perform the procedure described in "Collect Maintenance Data" on page 102.						
Event Data:	Byte **0** = FRU code as follows: **02** = CTP card, **05** = cooling fan, **06** = power supply assembly. Byte **1** = FRU slot number.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔				✔	

Table 48: Event Code 410

Message:	Switch reset.						
Severity:	Informational.						
Explanation:	The switch reset due to system power-up, IML, or manual reset. A software reset can occur automatically after a firmware fault (event code **411**), or be user-initiated. Event data indicates the type of reset.						
Action:	No action required.						
Event Data:	Byte **0** = reset type as follows: **00** = power-on, **02** = IML, **04** = reset.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔						

Table 49: Event Code 411

Message:	Firmware fault.						
Severity:	Major.						
Explanation:	Switch firmware encountered an unexpected condition and dumped operating state information to FLASH memory for retrieval and analysis. The dump file automatically transfers from the switch to the server, where it is stored for later retrieval through the data collection procedure. The switch performs a software reset, during which all attached Fibre Channel devices are momentarily disrupted, log out, and log back in.						
Action:	Perform the procedure described in "Collect Maintenance Data" on page 102.						
Event Data:	Bytes **0** through **3** = fault identifier, least significant byte first.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔				✔	

Table 50: Event Code 412

Message:	CTP watchdog timer reset.						
Severity:	Informational.						
Explanation:	The hardware watchdog timer expired and caused the CTP card to reset.						
Action:	Perform the procedure described in "Collect Maintenance Data" on page 102.						
Event Data:	Byte **0** = reset type as follows: **00** = task switch did not occur within approximately one second, **01** = interrupt servicing blocked for more than approximately one second.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔						

Table 51: Event Code 421

Message:	Firmware download complete.						
Severity:	Informational.						
Explanation:	A switch firmware version was downloaded from the embedded web server. The event data indicates the firmware version in hexadecimal format `xx.yy.zz bbbb`, where `xx` is the release level, `yy` is the maintenance level, `zz` is the interim release level, and `bbbb` is the build ID.						
Action:	No action required.						
Event Data:	Bytes **0** and **1** = release level (`xx`). Byte **2** = always a period. Bytes **3** and **4** = maintenance level (`yy`). Byte **5** = always a period. Bytes **6** and **7** = interim release level (`zz`). Byte **8** = always a space. Bytes **9** through **12** = build ID (`bbbb`).						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔						

Table 52: Event Code 423

Message:	CTP firmware download initiated.						
Severity:	Informational.						
Explanation:	The EWS interface initiated download of a new firmware version to the switch.						
Action:	No action required.						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔						

Table 53: Event Code 426

Message:	Multiple ECC single-bit errors occurred.						
Severity:	Minor.						
Explanation:	When the SDRAM controller detects an error checking and correction (ECC) error, an interrupt occurs. If an interrupt occurs a certain number of times weekly, a **426** event code is recorded. The number of interrupts is indicated by the event data.						
Action:	No action required. SDRAM is probably malfunctioning intermittently.						
Event Data:	Byte **0** of the event data (equal to **5**, **10**, **15**, or **20**) is recorded. The number of interrupts equals two to the power of the event data. Event data equal to **10** indicates 1,024 ECC error interrupts.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔						

Table 54: Event Code 433

Message:	Non-recoverable Ethernet fault.						
Severity:	Major.						
Explanation:	A non-recoverable Ethernet interface failure was detected and the LAN connection to the Ethernet network was terminated. No failure information or event codes are reported outside the switch. Although Fibre Channel port functionality is not affected, the switch cannot be monitored or configured.						
Action:	Replace the switch.						
Event Data:	Byte **0** = LAN error type as follows: **01** = hard failure, **04** = registered fault. Byte **1** = LAN error subtype (internally defined). Byte **2** = LAN fault identifier (internally defined).						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔				✔	

Table 55: Event Code 440

Message:	Embedded port hardware failed.						
Severity:	Major.						
Explanation:	The embedded port hardware detected a fatal CTP error.						
Action:	Replace the switch.						
Event Data:	Byte **0** = CTP slot position (**00**). Byte **1** = engineering reason code Bytes **4** through **7** = elapsed millisecond tick count.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔				✔	

Table 56: Event Code 442

Message:	Embedded port anomaly detected.						
Severity:	Informational.						
Explanation:	The switch detected a deviation in the normal operating mode or status of the embedded port.						
Action:	No action required. An additional event code is generated if this incident exceeds an error threshold or results in a port failure.						
Event Data:	Byte **0** = port number. Byte **1** = engineering reason code. Bytes **4** through **7** = elapsed millisecond tick count. Bytes **8** and **9** = high-availability error callout #1. Bytes **10** and **11** = high-availability error callout #2. Byte **12** = detecting port. Byte **13** = connected port. Bytes **16** and **17** = high-availability error callout #3. Bytes **18** and **19** = high-availability error callout #4.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔						

Table 57: Event Code 445

<table>
<tr><td>Message:</td><td colspan="7">ASIC detected a system anomaly.</td></tr>
<tr><td>Severity:</td><td colspan="7">Informational.</td></tr>
<tr><td>Explanation:</td><td colspan="7">The application-specific integrated chip (ASIC) detected a deviation in the normal operating mode or operating status of the switch.</td></tr>
<tr><td>Action:</td><td colspan="7">No action required. An additional event code is generated if this incident exceeds an error threshold that results in a system event.</td></tr>
<tr><td>Event Data:</td><td colspan="7">Byte 0 = port number.
Byte 1 = engineering reason code.
Bytes 4 through 7 = elapsed millisecond tick count.
Bytes 8 and 9 = high-availability error callout #1.
Bytes 10 and 11 = high-availability error callout #2.
Byte 12 = detecting port.
Byte 13 = connected port.
Bytes 16 and 17 = high-availability error callout #3.
Bytes 18 and 19 = high-availability error callout #4.</td></tr>
<tr><td rowspan="3">Distribution:</td><td colspan="2">Switch</td><td colspan="3">HAFM Server</td><td colspan="2">Host</td></tr>
<tr><td>EWS Event Log</td><td>System Error LED</td><td>Event Log</td><td>E-Mail</td><td>Call Home</td><td>Sense Info</td><td>Link Incident</td></tr>
<tr><td>✔</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

Table 58: Event Code 453

Message:	New feature key installed.						
Severity:	Informational.						
Explanation:	This event occurs when a new feature key is installed from the EWS interface. The switch performs an IPL when the feature key is enabled. Event data indicates which feature or features are installed.						
Action:	No action required.						
Event Data:	Byte **0** = feature description as follows: **00** through **04** = Flexport, **06** = open-system management server. Byte **1** = feature description as follows: **06** = SANtegrity Binding, **07** = Open Trunking						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔						

Port Events (500 through 599)

Table 59: Event Code 506

<table>
<tr><td>Message:</td><td colspan="7">Fibre Channel port failure.</td></tr>
<tr><td>Severity:</td><td colspan="7">Major.</td></tr>
<tr><td>Explanation:</td><td colspan="7">A Fibre Channel port failed. The amber LED corresponding to the port illuminates to indicate the failure. Other ports remain operational, if their LEDs are extinguished.</td></tr>
<tr><td>Action:</td><td colspan="7">Perform the procedure described in “Collect Maintenance Data” on page 102.
Perform a switch reset. If the problem persists, replace the switch.</td></tr>
<tr><td>Event Data:</td><td colspan="7">Byte 0 = port number (00 through 11).
Byte 1 = engineering reason code.
Bytes 4 through 7 = elapsed millisecond tick count.
Bytes 8 through 11 = reason code specific.
Byte 16 = connector type.
Bytes 17 and 18 = transmitter technology.
Byte 19 = distance capabilities.
Byte 20 = supported transmission media.
Byte 21 and 22 = speed capability and configuration.</td></tr>
<tr><td rowspan="3">Distribution:</td><td colspan="2">Switch</td><td colspan="3">HAFM Server</td><td colspan="2">Host</td></tr>
<tr><td>EWS Event Log</td><td>System Error LED</td><td>Event Log</td><td>E-Mail</td><td>Call Home</td><td>Sense Info</td><td>Link Incident</td></tr>
<tr><td>✔</td><td>✔</td><td></td><td></td><td></td><td>✔</td><td></td></tr>
</table>

Table 60: Event Code 507

Message:	Loopback diagnostics port failure.						
Severity:	Informational.						
Explanation:	A loopback diagnostic test detected a Fibre Channel port failure.						
Action:	No action required. An event code **506** is generated if this diagnostic failure results in a hard port failure.						
Event Data:	Byte **0** = port number (**00** through **11**). Byte **1** = engineering reason code. Bytes **4** through **7** = elapsed millisecond tick count. Bytes **8** through **11** = reason code specific. Byte **12** = test type.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔						

Table 61: Event Code 508

Message:	Fibre Channel port anomaly detected.
Severity:	Informational.
Explanation:	The switch detected a deviation in the normal operating mode or status of the indicated Fibre Channel port.
Action:	No action required. An event code **506** is generated if this anomaly results in a hard port failure.
Event Data:	Byte **0** = port number (**00** through **11**). Byte **1** = anomaly reason code. Bytes **4** through **7** = elapsed millisecond tick count. Bytes **8** and **9** = high-availability error callout #1. Bytes **10** and **11** = high-availability error callout #2. Byte **12** = detecting port. Byte **13** = connected port. Bytes **16** and **17** = high-availability error callout #3. Bytes **18** and **19** = high-availability error callout #4.

Table 61: Event Code 508 (Continued)

Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Table 62: Event Code 510

Message:	SFP optical transceiver hot-insertion initiated.						
Severity:	Informational.						
Explanation:	Installation of a small form factor pluggable (SFP) optical transceiver was initiated with the switch powered on and operational. The event indicates that operational firmware detected the presence of the transceiver.						
Action:	No action required.						
Event Data:	Byte **0** = port number (**00** through **11**). Bytes **4** through **7** = elapsed millisecond tick count.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔						

Table 63: Event Code 512

Message:	SFP optical transceiver nonfatal error.						
Severity:	Minor.						
Explanation:	Switch firmware detected an SFP optical transceiver non-fatal error.						
Action:	Replace the failed transceiver with a functional transceiver of the same type.						
Event Data:	Byte **0** = port number (**00** through **11**). Byte **1** = engineering reason code. Bytes **4** through **7** = elapsed millisecond tick count.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔						

Table 64: Event Code 513

Message:	SFP optical transceiver hot-removal completed.						
Severity:	Informational.						
Explanation:	An SFP optical transceiver was removed while the switch was powered on and operational.						
Action:	No action required.						
Event Data:	Byte **0** = port number (**00** through **11**). Bytes **4** through **7** = elapsed millisecond tick count.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔						

Table 65: Event Code 514

Message:	SFP optical transceiver failure.						
Severity:	Major.						
Explanation:	An SFP optical transceiver failed. The amber LED corresponding to the port illuminates to indicate the failure. Other ports remain operational if their LEDs are extinguished.						
Action:	Replace the failed transceiver with a functional transceiver of the same type.						
Event Data:	Byte **0** = port number (**00** through **11**). Byte **1** = engineering reason code. Bytes **4** through **7** = elapsed millisecond tick count.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔				✔	

Table 66: Event Code 523

Message:	FL_Port open request failed.						
Severity:	Informational.						
Explanation:	When the indicated FL_Port attempted to open a loop device, the port open (OPN) sequence was returned.						
Action:	No action required.						
Event Data:	Byte **0** = port number (**00** through **11**). Byte **1** = arbitrated loop physical address (AL_PA) of the device transmitting the OPN sequence.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔						

Table 67: Event Code 524

Message:	No AL_PA acquired.						
Severity:	Informational.						
Explanation:	Switch cannot allocate an AL_PA of **0** (loop master) for an FC-AL device during loop initialization. The device cannot participate in loop operation.						
Action:	Disconnect the FC-AL device that is loop master.						
Event Data:	Byte **0** = port number (**00** through **11**).						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔						

Table 68: Event Code 525

Message:	FL_Port arbitration timeout.						
Severity:	Informational.						
Explanation:	A switch port could not win loop arbitration within the specified loop protocol time out value (LP_TOV).						
Action:	Switch firmware reinitializes the arbitrated loop. No user action required.						
Event Data:	Byte **0** = port number (**00** through **11**).						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔						

Table 69: Event Code 581

Message:	Implicit incident.						
Severity:	Major.						
Explanation:	The event caused an implicit Fibre Channel link incident.						
Action:	A link incident record (LIR) is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. Go to "MAP 0000: Start MAP" on page 30 to perform fault isolation.						
Event Data:	Refer to the T11/99-017v0 document for the specific link incident record format.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
							✔

Table 70: Event Code 582

Message:	Bit error threshold exceeded.						
Severity:	Major.						
Explanation:	The number of code violation errors recognized exceeded the bit error threshold.						
Action:	An LIR is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. Go to "MAP 0000: Start MAP" on page 30 to perform fault isolation.						
Event Data:	Refer to the T11/99-017v0 document for the specific link incident record format.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
							✔

Table 71: Event Code 583

Message:	Loss of signal or loss of synchronization.						
Severity:	Major.						
Explanation:	A loss-of-signal condition or a loss-of-synchronization condition persisted for more than the specified receiver-transmitter timeout value (R_T_TOV).						
Action:	An LIR is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. Go to "MAP 0000: Start MAP" on page 30 to perform fault isolation.						
Event Data:	Refer to the T11/99-017v0 document for the specific link incident record format.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
							✔

Table 72: Event Code 584

Message:	Not operational primitive sequence received.						
Severity:	Major.						
Explanation:	A not-operational primitive sequence (NOS) was received.						
Action:	An LIR is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. Go to "MAP 0000: Start MAP" on page 30 to perform fault isolation.						
Event Data:	Refer to the T11/99-017v0 document for the specific link incident record format.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
							✔

Table 73: Event Code 585

Message:	Primitive sequence timeout.						
Severity:	Major.						
Explanation:	Either a link reset (LR) protocol timeout or a timeout while waiting for the appropriate response (while in a NOS receive state and after NOS was no longer recognized) occurred.						
Action:	An LIR is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. Go to "MAP 0000: Start MAP" on page 30 to perform fault isolation.						
Event Data:	Refer to the T11/99-017v0 document for the specific link incident record format.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
							✔

Table 74: Event Code 586

Message:	Invalid primitive sequence received for current link state.						
Severity:	Major.						
Explanation:	Either a link reset (LR) or a link-reset response (LRR) sequence while in the wait-for-online sequence (OLS) state occurred.						
Action:	An LIR is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. Go to "MAP 0000: Start MAP" on page 30 to perform fault isolation.						
Event Data:	Refer to the T11/99-017v0 document for the specific link incident record format.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
							✔

Thermal Events (800 through 899)

Table 75: Event Code 810

Message:	High temperature warning (CTP card thermal sensor).						
Severity:	Major.						
Explanation:	The thermal sensor associated with a CTP card indicates the warm temperature threshold was reached or exceeded.						
Action:	Perform the procedure described in "Collect Maintenance Data" on page 102. Perform a switch reset. If the problem persists, replace the switch.						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error Indicator	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔				✔	

Table 76: Event Code 811

Message:	Critically hot temperature warning (CTP card thermal sensor).						
Severity:	Major.						
Explanation:	The thermal sensor associated with a CTP card indicates the hot temperature threshold was reached or exceeded.						
Action:	Perform the procedure described in "Collect Maintenance Data" on page 102. Perform a switch reset. If the problem persists, replace the switch.						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔				✔	

index

A

applications
  diagnostic features 18
  EWS interface 18
audience 10
authorized reseller, HP 14

B

block ports 106

C

conventions
  document 11
  equipment symbols 12
  text symbols 11
cooling fan
  fault isolation 52
CTP card
  event codes tables 151
  fault isolation 52
  firmware versions 113

D

document
  conventions 11
  prerequisites 10
  related documentation 10
download firmware 115

E

E_Port
feature key requirement 15
segmented 74
E_Port, description 15
electrostatic discharge (ESD)
repair procedures, caution 88
equipment symbols 12
error detection
description 17
event codes 26
EWS interface 18
error reporting
description 17
event codes 26
EWS interface 18
ESD
repair procedures, caution 88
event codes
CTP card events 151
description 129
fan module events 148
system events 131
thermal events 167
Event Log
description 89
EWS interface
default display 18
external loopback test
description 98
procedure 100

F

F_Port, description 15
fan module events, event codes tables 148
fault isolation
MAP 0000 - Start MAP 30
MAP 0100 - Power distribution analysis 41
MAP 0200 - POST failure analysis 44
MAP 0300 - Loss of web browser PC communication 46
MAP 0400 - FRU failure analysis 52
MAP 0500 - Port failure and link incident analysis 57
MAP 0600 - Fabric, ISL, and segmented port problem determination 74
summary 26
fiber-optic
cleaning kit 23
components, cleaning 108
protective plug 22
wrap plug 22
firmware 113
adding a version 114
determine version 113
download 115
FL_Port
description 15
FRU removal
SFP transceivers 122
tools required 122
FRU replacement
SFP transceiver 123
tools required 122
FRUs
front-accessible 126
illustrations 125
part numbers 125
SFP transceivers 126
full-volatility feature 102

G

G_Port 15
gateway address
default 25
getting help 14
GX_Port 15

H

help, obtaining 14
HP
  authorized reseller 14
  storage website 14
  technical support 14

I

illustrated parts breakdown 125
IML switch 111
internal loopback test
  description 98
  procedure 99
interswitch link
  description 15
  fault isolation 74
IP address
  default 25

L

laser transceiver
  removal 122
  replacement 123
LEDs
  port status 90
logs
  clear 89
  using information 89
loopback test
  description 98
  external 100
  internal 99

M

maintenance
  approach 21
  event codes 129
maintenance analysis procedures
  MAP 0000 - Start MAP 30
  MAP 0100 - Power distribution analysis 41
  MAP 0200 - POST failure analysis 44
  MAP 0300 - Loss of web browser PC communication 46
  MAP 0400 - FRU failure analysis 52
  MAP 0500 - Port failure and link incident analysis 57
  MAP 0600 - Fabric, ISL, and segmented port problem determination 74
  summary 26
modem cable 22

N

null modem cable 22

O

offline state, set 105
online state, set 104

P

part numbers 125
parts 125
password
  default 25
performance statistics
  Class 2 96
  Class 3 96
  errors 95
  traffic 95
ports
  block 106
  configurable types 15
  diagnostics 90
  loopback test 98
  performance statistics 94
  port properties 97
  port technology 97
  status LEDs 90
  unblock 106
power supply
  fault isolation 41
power-off procedure 110
power-on procedure 109

prerequisites 10
preventive maintenance, cleaning fiber-optic components 108
protective plug, fiber-optic 22

R

rack stability, warning 13
related documentation 10
repair procedures
  block or unblock a port 106
  collect maintenance data 102
  IML or reset the switch 111
  manage firmware versions 113
  obtain port diagnostic information 90
  perform port diagnostic loopback tests 98
  power-off procedure 110
  power-on procedure 109
  reset configuration data 118
  set the switch online or offline 104
repair, event codes 129
reset
  configuration data 118
  switch 112

S

segmented E_Port
  fault isolation 74
serviceability features 17
SFP transceivers
  fault isolation 57
  illustrations 126
  part numbers 126
  protective plug 22
  removal 122
  replacement 123
  wrap plug 22
SNMP
  description 20
  traps 20
software
  diagnostic features 18
  EWS interface 18
subnet mask
  default 25
switch
  description 15
  event codes 129
  FRUs, front accessible 126
  illustrated parts breakdown 125
  MAPs 25
  tools supplied 22
symbols in text 11
symbols on equipment 12
system error light, clear 89
system events
  event codes tables 131

T

technical support, HP 14
text symbols 11
thermal events, event codes tables 167
tools and test equipment 22
  FRU removal and replacement 122
tools, supplied by service personnel 23
tools, supplied with switch 22

U

unblock ports 107

W

warning
  rack stability 13
  symbols on equipment 12
websites
  HP storage 14
wrap plug, fiber-optic 22

Z

zones 81